1. PURPOSE

This policy has been created to ensure that the information technology services provided by Asis Elektronik ve Bilişim Sistemleri A.Ş. in the fields of software and smart city systems are:

Customer satisfaction and service quality-oriented,

Managed in accordance with information security principles,

Meeting the criteria of continuity, accessibility, and risk management,

Compliant with ISO/IEC 20000-1:2018 and ISO/IEC 27001 standards,

Continuously improved in terms of IT service processes.

2. SCOPE

This policy applies to:

Asis Elektronik ve Bilişim Sistemleri A.Ş.'s IT service management processes,

Information assets and infrastructure,

Internal and external customers,

All employees,

External suppliers and business partners.

This policy regulates all IT service management processes, including internal operations, customer services, and supply chain management.

3. CORE PRINCIPLES AND COMMITMENTS

3.1 Compliance with Service Management Standards

Full compliance with ISO/IEC 20000-1:2018 and ISO/IEC 27001 standards will be ensured.

Service management processes will be documented, reviewed, and continuously improved.

Customer commitments will be fulfilled in accordance with Service Level Agreements (SLAs).

3.2 Information Security

Security measures will be implemented against unauthorized access, data loss, and cyberattacks.

An Information Security Management System (ISMS) will be actively operated in compliance with ISO/IEC 27001.

All employees will undergo information security training to raise awareness.

Data backup, disaster recovery, and crisis management plans will be continuously updated.

3.3 Customer Focus

Customer feedback will be regularly analyzed, and improvement processes will be implemented.

24/7 customer support and maintenance services will be provided to guarantee service continuity.

Service interruptions and performance issues will be proactively identified and resolved.

3.4 Service Continuity

Backup, disaster scenarios, and business continuity plans will be established to prevent disruptions in IT services.

Emergency change management processes will be applied to ensure the uninterrupted operation of systems.

Redundant infrastructure systems will be used for critical services.

3.5 Risk Management and Continuous Improvement

Risk assessments will be conducted for IT services, risks will be identified, and preventive measures will be taken.

Incident management and improvement processes will be implemented to minimize system failures.

The security risks of external suppliers and business partners will be periodically reviewed.

3.6 Financial Control and Budgeting

A separate budget will be allocated for IT services, and cost management processes will be implemented.

Expenditures will be monitored, and service costs will be optimized.

The costs of outsourcing will be tracked and audited.

4. ROLES AND RESPONSIBILITIES

4.1 Top Management

Ensure the implementation and continuous improvement of this policy.

Allocate necessary resources and support the processes.

Monitor risk management and service continuity policies.

4.2 Information Technology (IT) Department

Manage and improve IT service processes.

Implement and update information security policies.

Respond promptly to service interruptions and system failures.

4.3 Employees

Adhere to this policy and comply with information security rules.

Use access privileges to IT systems according to the established rules.

Report potential security breaches and service interruptions to the IT team.

4.4 External Suppliers and Business Partners

Comply with the security standards specified in contracts.

Collaborate with the company on service continuity and information security matters.

5. REVIEW AND PUBLICATION

This policy will be reviewed and updated at least once a year.

The updated policy will be approved by Top Management and shared through internal communication systems.

The updated versions will be added to the company's official documentation system.

6. INTERNAL CONTROL, AUDIT, AND REPORTING

This policy will be audited at least once a year by the Compliance Unit, in accordance with internal control and audit activities.

Internal audit reports will be shared with Top Management.

Full compliance with ISO/IEC 20000-1:2018 and ISO/IEC 27001 audit processes will be ensured.

This policy has been approved by the Top Management of Asis Elektronik ve Bilişim Sistemleri A.Ş. and must be implemented by all employees and relevant parties.

1. **REFERANSLAR** / **REFERENCES**

- TS EN ISO 20000-1 Bilgi Teknolojisi Hizmet Yönetim Sistemleri-Gereksinimler md. 5.2

2. **REVİZYON TARİHÇESİ** / **REVISION HISTORY**