OSA SEC

Information Security

and

Data Protection Policy

2024

v.1.0

Information Security and Data Protection Policy

1. Introduction

Information security and data protection are core to OSISEC's responsibility in delivering trusted IT solutions. This policy outlines the governance and controls required to safeguard systems, data, and stakeholder trust.

2. Purpose

- Protect OSISEC's information assets from unauthorized access or damage.
- Minimize internal and external information security risks.
- Ensure compliance with GDPR, KVKK, ISO 27001, and other relevant standards.
- Establish a culture of security awareness across the organization and its partners.

3. Scope

This policy applies to:

- All employees, contractors, and third parties working with OSISEC.
- All systems, platforms, and services managed by OSISEC.
- All categories of data, including personal, sensitive, proprietary, and client data.

4. Governance

4.1 Leadership

- The Chief Information Security Officer (CISO) is responsible for policy enforcement and monitoring.
- Subject Matter Experts (SMEs) regularly update strategies in response to threat landscapes.

4.2 Accountability

- All staff must follow this policy and report incidents.
- Managers must ensure their teams implement security measures effectively.

5. Security Principles

- **Confidentiality**: Access restricted to authorized users.
- **Integrity**: Data accuracy and trustworthiness preserved.
- **Availability**: Reliable access to critical systems.

6. Key Controls

6.1 Access Control

- Role-based access control (RBAC)
- Multi-Factor Authentication (MFA)
- Just-In-Time (JIT) access

6.2 Data Protection

- Encryption (AES-256+)
- Data masking for test environments
- Data classification and tagging

6.3 Network Security

- Next-Gen Firewalls (NGFW)
- Zero Trust Architecture
- Regular penetration testing

6.4 Endpoint Protection

- Endpoint Detection & Response (EDR)
- Security configuration baselines
- Disable auto-run and unauthorized app usage

6.5 Application Security

- Secure SDLC with threat modeling and testing
- DevSecOps integration
- Web Application Firewalls (WAF)

6.6 Threat Monitoring

- Threat Intelligence Platforms
- Security Information and Event Management (SIEM)
- Continuous risk assessments

7. Incident Response & Continuity

- Maintain Incident Response Plans (IRP)
- Cybersecurity playbooks (e.g., ransomware, DDoS)
- Biannual disaster recovery testing

8. Awareness & Training

- Mandatory onboarding and quarterly refresher training
- Specialized training for sensitive roles
- Phishing simulations

9. Third-Party & Supply Chain

- Vendor cybersecurity agreements
- Third-party risk assessments and audits
- Monitoring supply chain dependencies

10. Compliance

- ISO/IEC 27001
- NIST Cybersecurity Framework
- GDPR and KVKK
- Other sector-specific laws

11. Continuous Improvement

- Policy review every 6 months
- Post-incident lessons learned
- Investment in modern defense technologies

12. Enforcement

- Non-compliance may result in disciplinary action
- Legal escalation for serious violations

13. Review Criteria

- Annual or upon major regulatory/technical change
- New systems/tools implementation
- Lessons from security events

14. Reporting

- **Incidents**: incident@osisec.com.tr within 24 hours
- **Whistleblower Protection**: Good faith reporting is protected

Approved by

CEO: Bulent KONUK
Approval Date: 28 November 2024