Business Ethics

and

Code of Conduct

2024

v.1.0

Business Ethics and Code of Conduct

Introduction

OSISEC Business Ethics and Code of Conduct (hereinafter referred to as "Code") establishes the principles, standards, and practices to be adhered to by all partners, contractors, subcontractors, and associates (collectively referred to as "Partners") engaging with OSISEC BILISIM YAZILIM TICARET LIMITED SIRKETI (hereinafter referred to as "Company") in the provision, development, deployment, or integration of cybersecurity tools and services. Compliance with this Code is mandatory and reflects a commitment to maintaining the highest levels of ethical, legal, and technical integrity in all professional dealings.

Core Principles

Partners must comply with all applicable local, national, and international laws and regulations, including but not limited to:

- **European Union (EU):**
  - o General Data Protection Regulation (GDPR) for European Union territories**.**
- **United States:**
  - o California Consumer Privacy Act (CCPA) for services involving Californian residents.
  - o NIST Cybersecurity Framework for federal or U.S.-based operations.
- **International:**
  - o ISO/IEC 27001 Standards for information security management systems.
- **Türkiye:**
  - o KVKK (Law on the Protection of Personal Data, Law No. 6698): Governs the processing and protection of personal data, aligning with GDPR principles.
  - o Turkish Penal Code (Articles 243–246): Addresses cybercrimes, including unauthorized access and data modification.
  - o National Cybersecurity Strategy and Action Plan: Guides compliance in critical infrastructure and cybersecurity operations.
  - o Regulations by the Information and Communication Technologies Authority (BTK): Oversee ICT and cybersecurity-related operations.
  - o E-Transformation Turkey Project: Establishes legal and technical standards for e-Government and digital business operations.

2. Commitment to Data Security

Partners are required to implement and maintain robust cybersecurity measures to protect sensitive data. This includes but is not limited to:

- **Encryption Standards:** All data in transit and at rest must be encrypted using industry-standard protocols (e.g., AES-256, TLS 1.3).

- **Access Control:** Restrict access to data and systems strictly to authorized personnel on a need-to-know basis.

- **Incident Response:** Establish and maintain a clear incident response plan to detect, report, and mitigate breaches within a maximum of 24 hours of discovery.

Failure to uphold these standards constitutes a breach of this Code and will result in immediate review of the partnership agreement.

3. Ethical Use of Cybersecurity Tools

Partners are expressly prohibited from using cybersecurity tools provided by the Company to:

- Conduct illegal surveillance or monitoring.

- Violate individuals' privacy rights.

- Exploit vulnerabilities for unauthorized gain or activities.

All tools must be utilized solely for the purposes outlined in the agreement with the Company, ensuring transparency and ethical handling.

Technical and Operational Standards

4. System Integrity and Testing

Partners are obligated to ensure the integrity of all systems by:

- **Performing Regular Vulnerability Assessments:** Conduct bi-annual assessments to identify and mitigate weaknesses in systems and tools.

- **Penetration Testing:** Partners must engage certified professionals to perform annual penetration tests, ensuring real-world resilience.

- **Software Patching:** Apply updates and patches to tools and systems promptly, in alignment with manufacturer recommendations and cybersecurity best practices.

5. Confidentiality and Data Protection

The following measures must be observed to safeguard sensitive data:

- **Non-Disclosure Agreements (NDAs):** All personnel involved in handling sensitive data must sign and adhere to NDAs.
- **Data Minimization:** Collect and retain only the minimum amount of data required to perform contractual obligations.
- **Secure Data Disposal:** Implement secure data disposal methods, such as degaussing or shredding of physical media and certified deletion protocols for electronic data.

6. Supply Chain Security

Partners must evaluate and monitor the security practices of their own suppliers and subcontractors. This includes:

- Ensuring subcontractors comply with the same legal and ethical standards outlined in this Code.
- Avoiding sourcing components or software from untrusted or sanctioned entities.
- Conducting due diligence on supply chain entities before engagement.

Professional Conduct

7. Anti-Corruption and Fair Competition

Partners must uphold principles of fair competition and shall not engage in or tolerate:

- **Bribery or Kickbacks:** Offering, receiving, or soliciting anything of value to influence decisions.
- **Conflict of Interest:** Disclose any relationships or activities that could result in a conflict of interest.
- **Anti-Competitive Practices:** Manipulating market conditions or colluding with competitors.

8. Respect for Human Rights

Partners shall uphold internationally recognized human rights, including but not limited to:

- **Avoiding Discrimination:** Ensure equal opportunity and fairness in employment practices.
- **Labor Standards:** Adherence to child labor laws, forced labor prohibitions, and equitable working conditions.

9. Transparency and Reporting

All engagements with the Company must be transparent. Partners are required to:

- **Submit Accurate Documentation:** All reports, certifications, and invoices must be truthful and accurate.
- **Proactively Report Misconduct:** Notify the Company of any known or suspected violations of this Code or applicable laws without fear of retaliation.

Training and Continuous Improvement

10. Mandatory Training

Partners must ensure all relevant personnel complete annual training programs covering:

- **Cybersecurity Awareness:** Educating employees about phishing, social engineering, and malware threats.

- **Data Privacy:** Training on relevant data protection laws, secure handling practices, and rights of data subjects.
- **Ethical Standards:** Reinforcing the importance of integrity and ethical decision-making.

11. Continuous Improvement Initiatives

Partners are encouraged to engage in continuous improvement by:

- Adopting emerging technologies to enhance cybersecurity resilience.
- Collaborating with the Company to share insights, innovations, and best practices.
- Participating in audits and reviews to identify opportunities for enhancement.

Enforcement and Accountability

12. Monitoring and Audits

The Company reserves the right to:

- Conduct periodic audits of Partners' compliance with this Code.
- Require submission of third-party audit reports for cybersecurity standards.
- Perform random inspections to verify compliance with ethical and technical requirements.

13. Non-Compliance and Remediation

In cases of non-compliance, the following actions may be taken:

- **Immediate Suspension:** Temporary suspension of the partnership until the issue is resolved.
- **Termination of Contract:** Permanent termination in cases of egregious or repeated violations.
- **Legal Action:** Pursue remedies under applicable law for damages caused by non-compliance.

Acknowledgment and Acceptance

All employees, contractors and business partners must acknowledge their understanding and acceptance of this Code by signing the Annex-A - Acknowledgement of Receipt and Agreement. Failure to sign and return the acknowledgment will preclude any engagement or continuation of services.

Conclusion

This Code underscores the mutual commitment to ethical, secure, and lawful practices in delivering cybersecurity tools and services. By adhering to these principles, Partners contribute to a trustworthy and robust cybersecurity ecosystem, safeguarding the interests of all stakeholders.

Approved by

CEO: Bulent KONUK
Approval Date: 28 November 2024

Annex-A: Acknowledgement of Receipt and Agreement

By signing below, I affirm that I have read, understood, and agree to abide by the terms outlined in this OSISEC Business Ethics and Code of Conduct.

Partner Name: _____
Authorized Representative: _____

Signature: _____
Date: _____