DIGITECH AM LLC – Information Security Policy

1. Purpose

The purpose of this Information Security Policy is to establish a comprehensive framework for safeguarding DIGITECH AM LLC's information assets and ensuring the secure delivery of services related to remote gaming and bet collection operations. The policy is designed to protect the confidentiality, integrity, and availability of all information handled by the company, in full compliance with applicable Armenian laws, international standards, and industry best practices, including ISO/IEC 27001:2024. By implementing this framework, DIGITECH AM LLC demonstrates its commitment to mitigating risks, preventing unauthorized access, and maintaining trust with clients, users, and partners.

2. Scope

This policy applies to all individuals who interact with DIGITECH AM LLC's information systems, platforms, and databases. This includes employees, contractors, consultants, and third-party service providers who have access to operational or sensitive data. It covers all aspects of information management, from data creation and storage to processing, transmission, and disposal, ensuring that all activities related to remote gaming and bet collection operations are carried out securely and in accordance with regulatory obligations.

3. Governance

The governance of information security at DIGITECH AM LLC is under the ultimate responsibility of the Management, which ensures that policies and procedures are properly implemented and regularly updated. A designated Information Security Officer (ISO) oversees the day-to-day enforcement of security controls, risk assessments, and compliance with regulatory requirements. All employees and stakeholders are expected to understand their responsibilities regarding information security, promptly report potential security incidents, and adhere to established procedures to safeguard the company's assets and operations.

4. Information Classification

All information handled by DIGITECH AM LLC is classified according to its sensitivity. Highly confidential data includes customer information, internal operational metrics, and financial information. Operational procedures, internal communications, and company policies are considered internal use information, while publicly available materials, such as marketing content, are classified as public information. This classification ensures that appropriate security measures are applied based on the criticality of the information and the potential impact of unauthorized access or disclosure.

5. Risk Management

DIGITECH AM LLC adopts a proactive approach to risk management, regularly assessing potential threats to its systems, data, and operational processes. Risk assessments are conducted to identify vulnerabilities, evaluate potential impacts, and implement controls to mitigate identified risks. The company establishes a risk tolerance framework that aligns with its strategic objectives and regulatory requirements, and continuously monitors and reviews the effectiveness of security controls to maintain a secure operational environment.

6. Access Control

Access to DIGITECH AM LLC's information systems is strictly controlled and granted on a need-to-know basis, ensuring that employees and third parties can only access the information necessary for their role. Critical systems are protected through authentication and authorization mechanisms, including multi-factor authentication for administrative accounts. Privileged access is reviewed regularly, and any access no longer required is promptly revoked to prevent unauthorized use or data breaches.

7. Data Protection

DIGITECH AM LLC handles all customer and operational data in strict compliance with Armenian data protection legislation and GDPR principles where applicable. Personal data, including betting information, is encrypted both in transit and at rest, and data retention practices follow legal, regulatory, and operational requirements. These measures ensure that sensitive information is protected against loss, unauthorized access, or accidental disclosure, reinforcing the trust of clients and regulatory authorities.

8. Asset Management

All IT assets, including servers, databases, applications, and endpoints, are inventoried, classified, and managed throughout their lifecycle. Assets are maintained, updated, and securely disposed of when no longer in use to prevent unauthorized access or data leakage. This approach guarantees that the company's technological infrastructure remains secure, reliable, and aligned with operational needs.

9. Physical Security

Physical security measures are applied to offices, data centers, and other locations where critical systems and information are stored. Controlled access, surveillance systems, and environmental protection measures are in place to prevent unauthorized entry and to protect against environmental threats. Visitor access is strictly monitored and limited to authorized personnel, ensuring that the physical environment supports the company's overall security objectives.

10. Network and System Security

DIGITECH AM LLC implements robust technical measures to secure its networks and systems. Firewalls, intrusion detection systems, and anti-malware solutions protect against external threats, while regular patching and vulnerability management processes ensure that software and hardware remain secure and up to date. Network segmentation is applied to isolate critical gaming operations from less sensitive systems, reducing the risk of disruption or compromise.

11. Incident Management

All security incidents, including data breaches, unauthorized access attempts, or system failures, must be reported promptly through established internal procedures. A formal incident response plan defines the methods for containment, mitigation, recovery, and post-incident review. This ensures that incidents are managed efficiently, minimizing operational impact and preventing recurrence.

12. Business Continuity

DIGITECH AM LLC maintains comprehensive business continuity plans to guarantee uninterrupted remote gaming services and bet collection operations. Backup systems are regularly tested, and critical system redundancies are implemented to minimize downtime in the event of hardware failure, cyber-attack, or other disruptive incidents. These measures ensure that the company can continue providing reliable services even under adverse conditions.

13. Supplier and Third-Party Management

All third-party providers, including hosting and software partners, are required to comply with DIGITECH AM LLC's security standards. Regular audits and assessments are conducted to verify that suppliers maintain adequate security practices, ensuring that third-party interactions do not compromise the confidentiality, integrity, or availability of the company's information assets.

14. Training and Awareness

DIGITECH AM LLC invests in continuous training and awareness programs for all employees, ensuring that they understand information security, data protection, and regulatory compliance requirements. Staff are encouraged to actively participate in security initiatives, report potential threats, and contribute to the ongoing improvement of the company's security posture.

15. Policy Review

This Information Security Policy is reviewed periodically, or whenever significant changes occur in operations, technology, or legal requirements. Updates are communicated to all employees, contractors, and relevant stakeholders, ensuring that the policy remains current, effective, and aligned with the company's strategic objectives.