

OPERATIONS MANUAL

Ex Lux N.V.

Document Control

Version	Date	Description of Changes	Author
1.0	01.07.2026	Initial draft	IGA Group B.V.

OPERATIONS MANUAL

1. PURPOSE

This Operations Manual sets out the operational, technical, compliance, security, and responsible gaming framework implemented by **Ex Lux N.V.** in relation to its online gaming operations.

The purpose of this document is to demonstrate the systems, controls, and procedures implemented to ensure compliance with applicable Curaçao Gaming Authority (CGA) requirements, applicable gaming legislation, license conditions, and regulatory obligations.

2. COMPANY INFORMATION

2.1 Legal Entity

Company Name: Ex Lux N.V.

Registration Number: 164858

Registered Address: Zuikertuintjeweg Z/N, Curacao

Contact Details: support@takbet.com

Website(s):

Takbet.com

betfa.com

2.2 Key Persons

Position	Name	Contact
Director	IGA Trust B.V.	Contact@igatrust.com
CEO	Bryony Whitmore	BryonyWhitmore@protonmail.com
CCO/MLRO	Raffaele Magliulo	raffaele.magliulo.mlro@gmail.com
CTO	Markiyan Shevchenko	MarkiyanShevchenko@protonmail.com
CFO	Elia Marchetti	EliaMarchetti@protonmail.com

3. DESCRIPTION OF GAMING OPERATIONS

3.1 Games Offered

The Licensee offers online gaming products through approved gaming providers and systems. All gaming content is supplied and operated in accordance with applicable regulatory requirements.

Game Provider	Type of Games
[Provider Name]	[Slots / Live Casino / Table Games / Other]
[Provider Name]	[Slots / Live Casino / Table Games / Other]

3.2 Payment Methods

The Licensee supports the following payment methods:

Deposits

- Credit/Debit Cards
- Bank Transfer
- E-wallets
- Cryptocurrency (where applicable)

Withdrawals

- Bank Transfer
- E-wallets
- Other approved payment methods

All payment processing activities are monitored and performed through approved payment service providers in accordance with applicable AML/CFT requirements.

3.3 Betting Limits

The Licensee applies predefined betting limits to ensure responsible gaming controls and operational integrity.

Product	Minimum Bet	Maximum Bet
Casino	[\$0.10]	[\$1,000]
Sportsbook	[\$1]	[\$5,000]

3.4 Payout Procedures

The Licensee applies controlled payout procedures to ensure accurate settlement of gaming transactions.

Winning outcomes are determined through approved gaming systems and settlement procedures. Payout calculations are automatically generated based on the applicable game rules, betting conditions, and approved configurations.

Withdrawals are reviewed and approved through established operational and compliance controls before funds are released.

Applicable payment timelines are communicated to players through the Terms and Conditions and payment information pages.

3.5 Gaming Software

The Licensee operates using approved gaming technology and supporting systems.

System / Service	Provider
Gaming Platform Provider	[Digitain]
Sportsbook Provider	[Digitain]
Back-office Systems	[Digitain]
Certification Laboratories	[GLI]

3.6 Outcome Determination

Gaming outcomes are determined through certified gaming systems and approved random number generation processes.

The Licensee ensures:

- RNG systems operate according to certified methodologies;
- Sportsbook results are settled according to predefined rules;
- Third-party data feeds are obtained from approved providers;

- Game fairness controls are implemented and monitored.

4. QUALITY ASSURANCE AND TESTING

4.1 Testing Schedule

The Licensee performs regular testing and monitoring activities.

Test Type	Frequency	Responsible Person
RNG Testing	Quarterly	[Insert Responsible Person]
Penetration Testing	Annually	[Insert Responsible Person]
Vulnerability Scanning	Monthly	[Insert Responsible Person]
Backup Restoration Test	Quarterly	[Insert Responsible Person]

4.2 Quality Monitoring Methods

Quality assurance activities include:

- Internal operational reviews;
- Transaction monitoring;
- Security assessments;
- Software version management;
- Incident monitoring and review procedures.

5. PLAYER DATA MANAGEMENT

5.1 Data Collected

The Licensee collects and processes player information required for account management, regulatory compliance, AML/CFT obligations, and gaming operations.

Collected information includes:

- Name;
- Date of Birth;
- Address;
- Email;
- Phone Number;
- Payment Details;
- Transaction History.

5.2 Data Storage

Player data is stored securely using controlled production databases.

Data security controls include:

- Encryption of data in transit using [Insert Standard];
- Encryption of data at rest using [Insert Standard];
- Secure encryption key management through [Insert Provider/System].

Access to player data is restricted to authorised personnel only.

Access controls include:

- Role-based access management;
- Multi-factor authentication;
- User activity logging.

Player data is retained for the period required by applicable AML/CFT and regulatory requirements.

6. PLAYER INTERFACE

6.1 Website and Application Elements

The Licensee's player interface includes:

- Homepage;
- Registration process;
- Login functionality;
- Responsible Gaming section;
- Deposit and withdrawal pages;
- Bonus information pages.

Relevant screenshots and supporting materials are maintained as part of the licensing documentation package.

6.2 Mandatory Information Displayed

The player interface displays:

- License and company information;
- Responsible Gaming information;
- Terms and Conditions;
- Privacy Notice;
- Complaint handling and dispute resolution information.

7. PLAYER PROTECTION CONTROLS

7.1 Prohibited Players

The Licensee maintains controls preventing access by:

- **Self-excluded players** – Players who have voluntarily excluded themselves or have been excluded by the Licensee are blocked from logging in, creating new accounts, or participating in any gaming activity. Account checks are performed against the self-exclusion register during login and registration;
- **Underage persons** – Age verification procedures are applied at registration and before allowing withdrawals. Players must confirm they meet the minimum legal age requirement, and additional verification checks may be performed using third-party KYC tools;
- **Restricted jurisdictions** – IP detection, country verification, and payment instrument checks are used to prevent access from jurisdictions where services are prohibited or restricted under the applicable licence;
- **Sanctioned individuals** – The Licensee screens players against applicable international sanctions lists using automated compliance tools, and blocks or restricts accounts where a match or potential match is identified in accordance with AML/CFT obligations.

7.2 Verification Controls

Player verification procedures include:

- **KYC verification** – The Licensee applies Know Your Customer procedures at account registration and prior to enabling withdrawals, in order to verify the identity of each player and assess their eligibility to use the services;
- **Identity verification** – Players are required to submit valid identification documents (such as a passport, national ID card, or equivalent) which are checked for authenticity using automated and/or manual verification methods;
- **Age verification** – The Licensee confirms that all players meet the minimum legal age requirement before allowing full account activation or real-money play. Accounts suspected of belonging to underage individuals are suspended pending verification;
- **Enhanced Due Diligence (EDD) procedures where required** – Additional checks are performed on higher-risk players, including source of funds/wealth verification, increased transaction monitoring, and request for supplementary documentation in accordance with AML/CFT obligations.

7.3 Technical Controls

Technical safeguards include:

- **Geolocation monitoring** – The Licensee uses geolocation tools to determine the physical location of players and ensure they are accessing the platform only from permitted jurisdictions. Any inconsistencies between declared and detected locations may trigger further review or access restrictions;
- **IP monitoring** – IP addresses are monitored at login and during gameplay to identify suspicious activity, such as repeated access from restricted countries, use of anonymising services (e.g., VPNs or proxies), or abnormal login patterns;
- **Device fingerprinting** – The Licensee collects device-related information (such as browser type, operating system, device identifiers, and configuration data) to help identify returning users, detect fraudulent behaviour, and prevent misuse of multiple accounts;
- **Duplicate account detection** – Automated systems are used to identify potential duplicate accounts based on shared identifiers such as personal details, device fingerprints, IP addresses, payment methods, and behavioural patterns. Suspected duplicate accounts are reviewed and may be restricted or closed in accordance with the Terms and Conditions.

8. TECHNICAL INFRASTRUCTURE

8.1 Infrastructure Overview

The Licensee maintains documented technical infrastructure including:

- Network architecture;
- Data flow architecture;
- Server infrastructure.

8.2 Hosting Environment

Component	Location	Provider
Primary Servers		
Backup Servers		
Replication Server	Curaçao	Aquila B.V.

8.3 Security Controls

The Licensee implements and maintains a layered security framework designed to protect systems, data, and player information against unauthorized access, attacks, and misuse. This includes:

- **Firewalls** – Network firewalls are deployed to monitor and control incoming and outgoing traffic based on predefined security rules, ensuring only authorised traffic is permitted;
- **Web Application Firewall (WAF)** – A WAF is used to filter and monitor HTTP/HTTPS traffic between web applications and the internet, helping to prevent common application-layer attacks such as SQL injection and cross-site scripting (XSS);
- **DDoS Protection** – Distributed Denial of Service mitigation tools are in place to detect and absorb malicious traffic spikes, ensuring service availability and platform stability;
- **Access Management Controls** – Role-based access control (RBAC) is implemented to ensure that system and data access is restricted to authorised personnel only, following the principle of least privilege. Multi-factor authentication (MFA) is applied where appropriate for sensitive systems.

8.4 Disaster Recovery

The Licensee maintains documented backup and disaster recovery procedures to ensure business continuity and minimise data loss in the event of a system failure, cyber incident, or other disruptive event. These include:

- **Daily Backups** – Incremental backups of critical systems and databases are performed daily to capture recent changes;
- **Offsite Backup Storage** – Backup data is securely stored in geographically separate offsite environments to protect against localised failures or disasters;
- **Backup Integrity Checks** – Regular verification and testing of backups are performed to ensure data integrity and recoverability;
- **Recovery Procedures** – Defined recovery time objectives (RTO) and recovery point objectives (RPO) are maintained, and periodic disaster recovery tests are conducted to validate readiness.

8.5 Emergency Procedures

The Licensee maintains procedures covering:

- **System failures** – The Licensee has procedures in place to address unexpected system malfunctions, including application errors, software bugs, or infrastructure issues that may affect platform availability or performance. Critical systems are monitored to enable prompt detection, escalation, and recovery actions;
- **Data centre outages** – In the event of a data centre disruption or unavailability, services are designed to be restored through redundant infrastructure and failover mechanisms where applicable. Backup environments and recovery procedures are maintained to minimise downtime and data loss;
- **Cybersecurity incidents** – The Licensee maintains an incident response process to identify, contain, and remediate cybersecurity events such as unauthorised access, malware infections, data breaches, or denial-of-service attacks. Incidents are logged, investigated, and reported in line with internal procedures and regulatory requirements where applicable;
- **Business continuity events** – The Licensee prepares for broader disruptive events such as third-party service outages, critical staff unavailability, power failures, or other operational disruptions. Business continuity plans define roles, responsibilities, and recovery steps to ensure essential services can continue or be restored within acceptable timeframes.

9. RESPONSIBLE GAMING

Responsible Gaming measures are implemented in accordance with the Licensee's Responsible Gaming Policy.

The Responsible Gaming Policy is maintained as a separate controlled document and forms part of the Licensee's compliance framework.

10. TERMS AND CONDITIONS

Player Terms and Conditions governing the use of the gaming platform are maintained as a separate controlled document.

11. PLAYER COMPLAINTS AND DISPUTE RESOLUTION

The Licensee maintains formal complaint handling procedures in accordance with applicable regulatory requirements.

The Complaints Policy is maintained as a separate controlled document.

12. RECORD KEEPING

The Licensee maintains records relating to:

- Player information;
- Gaming activity including bets, wins, losses, and bonuses;
- Deposits, withdrawals, chargebacks, and financial transactions;
- AML/CFT documentation;
- Verification records.

All records are securely stored and retained for a minimum period of five (5) years or longer where required by applicable regulatory obligations.

All required information is available to the Curaçao Gaming Authority upon request through the Licensee's approved technical infrastructure