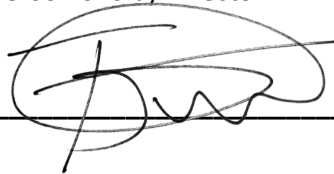


OPERATIONAL MANUAL of Game2Net B.V.

Date of effectiveness: 15.06.2026

Approved on: 15.06.2026 by Director

Prepared

A handwritten signature in black ink, consisting of a large, stylized 'V' followed by a series of loops and a horizontal stroke, positioned over a horizontal line.

**and
accepted by:**

**Vlasova Iryna
AML Officer/MRLO**

1. GENERAL

GAME2NET B.V. (the "Organisation") operates the COLDBET brand at coldbet.com under licence No. OGL/2024/296/1093 issued by the Curaçao Gaming Authority (the "CGA"). The Organisation is established under the laws of Curaçao, with its registered office at Abraham Mendez Chumaceiro Blvd. 03, Willemstad, Curaçao, CW000, and company number 163111.

This operational manual describes the manner and degree of the Organisation's compliance with the applicable gaming and financial-crime law, the licence conditions and the CGA's policies and guidelines, and the controls applied to ensure a safe, responsible, transparent, reliable and verifiable remote gambling operation. It is a working operating document: each section states who is responsible for an activity, when and how it is performed, by which control it is governed, where the resulting record is held, and how the activity is reviewed.

1.1 SCOPE AND APPLICATION

The manual applies to the entire remote gaming operation across all approved domains and subdomains, and binds all directors, key persons, employees and contractors involved in the operation. It is read together with the Organisation's Terms and Conditions and its underlying policies, in particular the AML/CFT and Sanctions Compliance Policy, the Responsible Gaming Policy, the Player Complaints Policy and the Dispute Resolution Policy. Where this manual summarises a matter governed in detail by one of those instruments, that instrument controls the operational detail; this manual records how compliance is organised and where the controlling procedure resides.

The controls described here are maintained as a foundational baseline that the Organisation operates and progressively matures over time. Where a control is delivered through a third-party platform, hosting provider or supplier, the Organisation remains fully responsible for the outcome and verifies delivery through contractual assurance, due-diligence assessment and ongoing monitoring; contractual delegation does not transfer the Organisation's accountability.

1.2 GOVERNANCE AND ACCOUNTABILITY

The Director holds ultimate executive responsibility for the operation and approves this manual and the underlying policies. The AML Officer/MLRO holds day-to-day responsibility for compliance, owns this manual, and serves as the compliance officer for unusual-transaction and identification purposes. Operational ownership of each control area is allocated to a named function so that, for every activity in this manual, a responsible owner can be identified. The allocation of control ownership is maintained in an internal responsibilities register kept current by the AML Officer/MLRO.

Executive responsibility for information-security oversight is assigned within the Organisation. Compliance with the policies and the effectiveness of the controls are subject to independent review on a recurring schedule, the results of which are reported to the Director, and corrective actions arising from any review are tracked to closure. Documented operating procedures are maintained for the key recurring activities, including access administration, backup and restore, logging and log review, change control and incident handling.

1.3 OWNERSHIP, MAINTENANCE AND REVIEW

The AML Officer/MLRO owns the manual and keeps it current with the operation at all times. The manual shall be reviewed at least twice a year, in June and January, and on any material change to the operation, the applicable law or the licence conditions. A material change includes the addition or removal of a game category or major supplier, a change of key person or ultimate beneficial owner, a change to the technical infrastructure or hosting arrangement, or a change required by the CGA.

Each review is recorded with the date, the reviewer and the resulting version, and superseded versions are retained for the retention period in Section 11. The manual is approved by the Director, and material amendments are notified to the CGA where notification or prior approval is required. The Organisation makes the manual available for CGA inspection within five working days of a request, and conforms it to any operational-manual template the CGA approves and publishes.

2. GAMES, SOFTWARE AND OUTCOME DETERMINATION

This section describes the games offered, the payment possibilities, bet amounts and payouts, the software used and the outcome-determining elements, and the controls that keep each of these accurate, certified and verifiable.

2.1 GAMES OFFERED

The Organisation offers the following categories of remote games of chance:

- Sports betting – fixed-odds betting on sporting events, pre-match and in-play;
- Casino – slots, table games and other casino games supplied by licensed third-party providers;
- Live casino – human-dealer table games streamed in real time from licensed studios;
- Virtual sports – software-simulated events supplied by Golden Race and Global Bet.

The complete games catalogue, the participating game providers, studios and aggregators, and the rules of each game are set out in the Terms and Conditions and on the platform. The Organisation offers no goods or services other than the licensed games of chance, and maintains an up-to-date inventory of its gaming equipment, gambling interface, application software and games, which is provided to the CGA on request. The inventory records, for each game and component, its title and variant, its version and the date it was made available, the supplying provider or aggregator, and its certification status; the inventory is reviewed at least twice a year and on any change to the catalogue, and the responsibility for keeping it current is allocated to a named function.

2.2 SOFTWARE AND OUTCOME DETERMINATION

Except for live-dealer games, game outcomes are determined by a Random Number Generator (RNG) that produces consistently random results, validated by running and analysing large volumes of game rounds. Live-dealer outcomes are determined by a physical event conducted under studio control and streamed

in real time. Sports and fixed-odds outcomes are determined by the real-world event and settled against the odds and market rules in force when the bet was accepted.

The Organisation works only with licensed software providers whose products are certified for soundness and integrity by a testing laboratory approved by the CGA. The Organisation does not alter the certified outcome-determining logic; configuration is limited to parameters that do not affect certified fairness, and any such configuration change is made under the change-control discipline in Section 3. Where games, the remote gaming server or game content are supplied by a third party, the Organisation verifies the supplier's certification status at the point of onboarding and at defined intervals thereafter, of at least once a year; requires, by contract, that the supplier maintain valid certification and notify the Organisation promptly of any lapse, withdrawal, scope change or pending renewal; notifies the CGA where it becomes aware that a supplier's certification has lapsed or been withdrawn for a component in use; and ceases to offer the affected content until valid certification is restored.

The rules of each game, the odds of winning, the method of determining the odds and, as far as possible, the payout percentage are made available to players, together with the total and any specific costs of participation.

2.3 STAKES AND PAYOUTS

The bet and payout parameters are as follows:

- Minimum stake on any single selection: \$0.30 / €0.20, or the currency equivalent;
- Maximum stake: set per selection, sport and event; for accumulators the lowest leg limit applies;
- Maximum return: €50,000, or the equivalent in another currency, per bet;
- Payment of winnings: within 30 calendar days of confirmation of the result.

Prize money is paid out in the same currency, virtual or fiat, used to play, and remains available to the player for not less than 30 months from the date it was awarded. Bets are accepted only up to the player's available balance and, once registered, cannot be altered or revoked. The Organisation does not extend credit for wagering. The conditions under which the distribution of player funds and winnings may be suspended, cancelled or declared invalid are set out in the Terms and Conditions, and any decision to suspend or withhold a distribution is recorded with its reason and the responsible approver.

2.4 DEPOSITS AND WITHDRAWALS

Deposits and withdrawals are made through the methods published on the platform, including payment cards, e-wallets, bank transfer, cash and cryptocurrency (Bitcoin). A service charge applies to deposits and withdrawals made in BTC through the Bitcoin payment system. Fiat currencies accepted as stakes are tradable on international markets, and virtual currencies accepted as stakes are tradable on internationally licensed virtual-currency exchanges.

Withdrawals are processed 24/7, are subject to limits of €10,000 per day, €30,000 per week and €100,000 per month, and are returned to the method used to deposit. All payment transactions between the Organisation and the player are carried out exclusively through the player account, for which the

Organisation maintains a separate account for player deposits and winnings, with appropriate ring-fencing and segregation so that funds are available at all times to pay out prize money. The Organisation does not exchange currencies in the player account or otherwise, does not exchange virtual currencies for fiat currencies, and does not offer investment alternatives to players.

Each deposit and withdrawal is recorded in the player account management system with its amount, currency, method, status and timestamps, so that any transaction can be traced back to the player and reconstructed. The acceptance, screening and rejection of payment methods are governed by the Organisation's internal compliance policies and procedures, and the operative criteria for those decisions reside in those policies and are not reproduced here.

3. TESTING AND QUALITY ASSURANCE

This section describes the periodic test methods used for quality monitoring and the process by which testing is triggered, owned, recorded and escalated.

3.1 CERTIFICATION

All games owned by the Organisation are certified for soundness and integrity by a testing laboratory approved by the CGA before they are offered, and games supplied by third parties are certified by a CGA-approved laboratory before being made available. The gaming equipment and application software comply with international standards and are tested for information security and integrity by an independent qualified entity approved by the CGA. Certification covers the correctness and unpredictability of the RNG, the conformity of game behaviour to the published rules and return-to-player, and the integrity of the result-determination and settlement chain.

For games, remote gaming servers and game content supplied by third parties, the obligation to obtain and maintain valid certification rests with the supplier. The Organisation verifies each supplier's certification status at onboarding and at least annually thereafter, records the verification and its outcome in the supplier register described in Section 7, and applies the cessation and notification steps in Section 2.2 where a certification is found to have lapsed or been withdrawn.

3.2 PERIODIC TESTING

The Organisation applies an ongoing testing regime, owned by a named technical function and overseen by the AML Officer/MLRO, that includes:

- re-verification of the RNG at regular intervals and on any change to it;
- monitoring of realised return-to-player against certified theoretical values, with investigation of material deviations and corrective action tracked to closure;
- regression and acceptance testing of any new game, game version or platform release before it goes live, performed in a non-production environment;

- periodic information-security and integrity testing, including vulnerability scanning and, where appropriate, independent assessment, by a qualified entity approved by the CGA;
- logging and review of game-engine and settlement errors, with each error recorded, triaged by impact and tracked to resolution.

3.3 CHANGE CONTROL AND MAINTENANCE

The Organisation maintains the gaming equipment, gambling interface and application software, and replaces or expands them as necessary to preserve the integrity of the operation. Changes to the production environment are subject to documented change control comprising assessment of the change and its risk, testing in a non-production environment, approval by the responsible owner, scheduling outside peak operating hours where practicable, recording of the approval and the deployment result, and the ability to roll back. Changes affecting certified fairness, the result-determination chain or critical data require re-certification or re-testing before deployment, and any critical change requires the prior permission of the CGA.

Configuration of systems is managed against documented secure-configuration standards, and configuration changes are made through the same change-control discipline so that the secure baseline is preserved. The change record forms part of the evidence retained under Section 11.

4. STORAGE OF PLAYERS' PERSONAL DATA

This section describes how players' personal data and other regulated information are classified, stored, protected, accessed and disposed of. Processing is carried out in accordance with applicable data-protection law and the privacy provisions of the Terms and Conditions, and the protections described here form a foundational information-security baseline that the Organisation maintains and progressively matures.

4.1 DATA HELD AND CLASSIFICATION

Personal data collected at registration and during the relationship is stored in an encrypted, password-protected database within the Organisation's secure network, behind active firewall protection, with data in transit protected by TLS encryption. The data held includes identification data; account credentials in protected form; identity and address verification records; financial data, including payment instruments and the record of deposits, withdrawals and balances; gaming data, including bets, stakes, results and session activity; responsible-gaming data, including limits and exclusion elections and records of player interactions; and communications and complaints records.

The Organisation operates a documented data-management process under which all data is classified by sensitivity, and handling, storage, sharing and disposal rules are defined for each class. The classes distinguish, at least, critical gaming data such as game outcomes and high-value events; player personal data such as identity documents, payment details and behavioural data; business-confidential information; and public information. For each class the process defines access restrictions, approved

storage locations and protections, permitted transfer methods and minimum and maximum retention. The classification scheme is reviewed at least annually and on any significant change to systems, processes or applicable law.

The Organisation maintains a central inventory of the locations where sensitive data is stored, processed or transmitted, covering on-premise and cloud storage, application servers and backup repositories, each labelled by data class. The inventory is kept current and is reviewed at least annually and on any significant change to the infrastructure.

4.2 SECURITY, ACCESS AND PROCESSING

Access to personal data is restricted to authorised personnel on a need-to-know basis under role-based access controls and the principle of least privilege. Access is granted through a documented, auditable process that requires approval by the responsible manager and is linked to the individual's role; access is reviewed periodically and is revoked promptly on a change of role or departure. Multi-factor authentication is required for remote access, for administrative access to core systems and for externally accessible applications. Administrative actions are performed over encrypted, authenticated management protocols, and default accounts and credentials are removed or secured. Activity on systems holding personal data is logged, and the logs are collected to protected, tamper-resistant storage and reviewed for anomalies.

Data is processed only for the purposes for which it was collected, including operation of the player account, compliance with legal and regulatory obligations, and player protection. Sensitive data is encrypted at rest and in transit using industry-standard protocols, and a key-management arrangement governs the generation, storage, use and retirement of cryptographic keys. Where player or financial data is used in development, testing or analytics, it is masked so that production personal data is not exposed. Customer due diligence and the handling of personal data for compliance purposes are carried out under the Organisation's internal compliance policies and procedures, whose operative criteria are not reproduced here.

4.3 RETENTION AND SECURE DISPOSAL

Records are retained for at least five years, or longer where required by law, calculated from the end of the business relationship or the date of the relevant transaction or communication. Retention schedules are defined for each data class in line with regulatory and operational requirements. On expiry of the applicable period, data is securely disposed of by cryptographic erasure, overwriting or physical destruction of media, as appropriate, unless a legal basis requires continued retention.

5. VISUAL ELEMENTS PRESENTED TO PLAYERS

This section describes the visual elements shown to players through the gaming website and applications, and gives effect to the publicly-accessible-information requirements.

5.1 PRINCIPAL INTERFACE ELEMENTS

The platform presents the following principal elements:

- a lobby with navigation to the sports, casino, live-casino and virtual-sports sections;
- game and event pages showing the rules, the odds, the method of determining the odds and, as far as possible, the payout percentage, with the total and any specific costs of participation;
- a registration and login flow, with access to the player account only after registration and login;
- an account dashboard showing the balance, the opening balance and total stake since the most recent login, transaction history and verification status;
- responsible-gaming controls, including the deposit-limit, cooling-off and self-exclusion tools and a session timer visible while the player is logged in;
- a footer stating that under-age gambling is prohibited and displaying the CGA digital seal, the licence details and links to the relevant policies;
- access to a detailed record of the player's betting history and to a responsible-gaming self-assessment tool.

Responsibility for keeping the publicly displayed information accurate and current is allocated to a named function, and changes to it are made through the change-control discipline in Section 3 so that the displayed content remains consistent with the Terms and Conditions and the underlying policies.

5.2 PUBLICLY ACCESSIBLE INFORMATION AND THE CGA SEAL

On the publicly accessible part of the interface, the Organisation provides correct and up-to-date information including the registered and trade name and the company number; a statement that the CGA is the licensing authority and supervisor; a reference to the Terms and Conditions; the prohibition of participation by minors and other vulnerable persons; information about gambling addiction and where to seek help; the complaints and disputes procedure; the period within which and the currency in which prize money is payable; and the means by which players can limit their participation or exclude themselves from play, registration and marketing. The CGA digital seal is displayed at all times in accordance with its applicable conditions.

5.3 LANGUAGE AND NOTIFICATION OF CHANGES

Information is provided in English and in other major languages for the ease of use by potential customers, in a manner that is appropriate, understandable and accessible. The Terms and Conditions are available for consultation at all times from any page of the publicly accessible interface. The Organisation informs players in a timely manner of changes to the publicly accessible information and the Terms and Conditions, drawing attention to the changes upon login so that the player can decide whether to continue playing.

6. PREVENTION OF PARTICIPATION BY PROHIBITED PERSONS

This section describes the technical and procedural measures that prevent prohibited persons from playing, who operates them and how the resulting events are recorded.

6.1 AGE VERIFICATION

Access to funded play is restricted to persons aged 18 or older. The platform displays a clear under-age prohibition, and age is confirmed through identity verification before funded play is permitted. Where age cannot be confirmed, the account is restricted from funded play and from withdrawals until verification is completed. Suspected participation by minors is handled as a protective and compliance matter under the Organisation's internal compliance policies and procedures, and each such case is recorded with the action taken.

6.2 GEO-RESTRICTION

Registration and play are blocked, by technical geo-restriction operating at registration and login, for persons located in or resident in the prohibited jurisdictions maintained under the Organisation's AML/CFT and Sanctions Compliance Policy. The controlling list and the underlying screening logic are maintained under that policy and are not reproduced in player-facing materials. The prohibited jurisdictions are:

Cuba, Iran, North Korea, Syria, Ukraine (Crimea, Donetsk, Luhansk), Russian Federation, Cote d'Ivoire, Congo, Eritrea, Iraq, Lebanon, Liberia, Libya, Somalia, Afghanistan, Burma (Myanmar), Central African Republic, Ethiopia, Sudan, Venezuela, Yemen, Zimbabwe, Australia, Austria, Belgium, Belize, Bulgaria, Colombia, Croatia, Curaçao, Denmark, Estonia, Finland, France, Georgia, Germany, Italy, Netherlands, Panama, Portugal, Romania, Spain, Sri Lanka, United Kingdom, United States, Aruba, Bonaire, Saba, Statia and St. Martin.

Furthermore, registration and play are blocked for persons located in or resident in restricted jurisdictions where the provision of Gaming Services is prohibited by CGA Licensing Conditions or applicable laws. These restricted jurisdictions are:

Ukraine, Antigua and Barbuda, Netherlands Antilles, Barbados, Belarus, British Virgin Islands, Vanuatu, Hungary, Gabon, Guinea, Guinea-Bissau, Guernsey, Hong Kong, Greece, Jersey, Israel, Canada, Cyprus, Kiribati, China, Latvia, Lithuania, Malta, New Zealand, Norway, Papua New Guinea, Poland, Puerto Rico, Slovakia, Slovenia, Tuvalu, Turkey, French Guiana, Czech Republic, Switzerland, Sweden, Equatorial Guinea, South Korea, Guam, American Samoa, Palau, Northern Mariana Islands, Channel Islands, Hawaii, U.S. Virgin Islands, Sint Maarten, and United States Minor Outlying Islands.

6.3 EXCLUDED PLAYERS AND DUPLICATE ACCOUNTS

Players who have self-excluded, or who have been excluded by the Organisation as a protective measure, are prevented from registering or playing for the duration of the exclusion. The Organisation takes measures to detect and prevent duplicate or linked accounts used to circumvent exclusions, limits or restrictions, including matching of identification, contact, device and payment indicators, and treats

detected circumvention as a protective and compliance matter. Detected exclusions and circumvention attempts are recorded in the player account management system with the indicators relied on and the action taken.

6.4 IDENTITY AND DUE-DILIGENCE GATE

Funded play is subject to identity verification and customer due diligence. The applicable acceptance, identification, verification and screening procedures, and the criteria that trigger any enhanced measures, are set out in the Organisation's internal compliance policies and procedures and are not reproduced here.

7. TECHNICAL INFRASTRUCTURE AND BUSINESS CONTINUITY

This section describes the technical infrastructure, the information-security controls applied to it, and the restoration arrangements for a technical emergency. The controls described here form a foundational security baseline that the Organisation operates and progressively matures, scaled to the nature of the operation. A diagram of the Organisation's technical infrastructure is included as Annex A to this manual and forms part of it, and is also provided to the CGA on request.

7.1 INFRASTRUCTURE OVERVIEW

The technical infrastructure comprises a player-facing web and application layer; an account and wallet layer, including the player account management system in which balances, transactions and responsible-gaming interactions are recorded; integrations with third-party game and payment providers; and a data layer holding player, gaming-transaction and financial-transaction records. Components are segmented, administrative access is restricted and logged, and data in transit and at rest is protected by encryption as described in Section 4.

7.2 ASSET MANAGEMENT

The Organisation maintains a complete and accurate inventory of the hardware and software assets that interact with gaming data or systems, including infrastructure and application servers, networking hardware, end-user computing devices and the software platforms, operating systems and security tools in use. For each asset the inventory records its identifier, its owner or responsible function, and its network and approval status; for software it records the title and version, the installation date and the associated business function. The asset inventory is reviewed at least twice a year, and unauthorised or unmanaged devices appearing on the network are identified and addressed under a documented procedure, with priority given to anything that could affect game fairness or the protection of player data. Software support status is checked periodically, and unsupported software is removed or, where an exception is justified, run under documented compensating controls.

7.3 SECURE CONFIGURATION

Systems and devices are deployed against documented secure-configuration standards based on recognised industry baselines and vendor hardening guidance, covering servers, endpoints, security appliances and network equipment. User devices lock automatically after a defined period of inactivity. Host-based firewalls are deployed with a default-deny posture, and rule changes are reviewed, approved and recorded. Administrative interfaces are accessed only over secure, authenticated protocols, and insecure protocols are disabled unless explicitly justified. Default accounts are disabled or renamed and default passwords are changed on deployment. The configuration standards are reviewed at least annually and on the introduction of new technology, and all configuration changes pass through the change control in Section 3 so that performance and certified fairness are preserved.

7.4 ACCOUNT AND ACCESS MANAGEMENT

The Organisation maintains an inventory of all user, service and administrative accounts and reviews it periodically to confirm that each account remains valid and necessary. Strong, unique passwords are enforced, shared and default passwords are prohibited, and dormant accounts are disabled after a defined period of inactivity. Privileged accounts are managed separately from ordinary user accounts. Access to systems and data is provisioned through a documented, manager-approved process tied to the individual's role, is revoked promptly on role change or departure, and is governed by least privilege and need-to-know. Multi-factor authentication is required for externally accessible applications, for remote access and for administrative access to core gaming and infrastructure systems. Access events are logged and auditable.

7.5 VULNERABILITY AND PATCH MANAGEMENT

The Organisation operates a documented, risk-based vulnerability-management process covering asset discovery, scanning on a regular cycle, risk evaluation and time-bound remediation across operating systems, network infrastructure, web applications and third-party software, informed by vendor advisories and threat intelligence. Patches and updates for operating systems, software and firmware are applied on a regular cycle through a repeatable process, tested in a non-production environment before deployment where practicable, scheduled to avoid disruption, and recorded with their approval and result. Remediation and patch activity are tracked to closure.

7.6 LOGGING AND MONITORING

Audit logging is enabled across the enterprise assets, and logs are collected to centralised, tamper-resistant storage with restricted access. Logging covers, at least, player activity and betting transactions, high-value and payout events, fund movements, and administrative access and configuration changes. The integrity of logs is protected, retention is defined in line with regulatory and business requirements, and logs are reviewed periodically for anomalies. The logging process is reviewed at least annually and on significant change to the systems or the operation.

7.7 MALWARE, WEB AND EMAIL THREAT PROTECTION

Centrally managed anti-malware tooling is deployed across endpoints and servers, configured for automatic updating and regular scanning, and verified for compatibility with the gaming systems. Only supported, current browsers and email clients are used, and DNS filtering is applied to block known malicious or unauthorised domains without impeding legitimate gaming connectivity. Where removable media is used, auto-execution is disabled and media is validated before any transfer of data.

7.8 NETWORK SECURITY

Network infrastructure is segmented and is maintained on current, supported firmware and software. An inventory of network devices is kept, firmware and software status is reviewed on a regular cycle, and updates are applied on the basis of vendor advisories and risk, with end-of-life products avoided in the live environment. Network changes are coordinated with maintenance windows and supplier support so that availability is preserved.

7.9 PHYSICAL AND HUMAN-RESOURCE SECURITY

Physical and environmental controls protect the facilities and equipment that support the operation, including restricted access to secure areas, entry logging, environmental safeguards such as power continuity, and clear-desk and clear-screen practices; equipment used or stored off premises is secured. Security responsibilities are managed across the employment lifecycle: background checks are applied to new joiners in critical or sensitive roles, with enhanced screening for those handling financial systems, player data or system oversight; confidentiality obligations are included in engagement terms; security responsibilities are acknowledged on joining; and on departure, access is disabled and assets are reclaimed promptly. The conduct of the workforce in security matters is reinforced through the training in Section 12.

7.10 THIRD-PARTY AND SERVICE-PROVIDER MANAGEMENT

The Organisation maintains a current inventory of its service providers and suppliers, including gaming software vendors, hosting and infrastructure providers, payment processors, content aggregators, sports-data-feed providers and remote-gaming-server and player-management-system providers. For each provider the inventory records the scope of services, the data and systems accessed, the internal owner, the contractual security and integrity obligations and the certification or audit status, together with the arrangements for detecting and responding to feed manipulation, integrity failures or service disruption. The Organisation remains fully responsible for compliance where it relies on a third party, verifies delivery through due diligence and ongoing monitoring, and does not procure critical services or goods from a supplier that is not entitled to provide them.

7.11 CRYPTOGRAPHIC CONTROLS AND DATA MASKING

Sensitive gaming, player and financial data is protected by cryptographic controls, encrypted at rest and in transit using industry-standard protocols, under a key-management arrangement covering the generation, storage, use and retirement of keys. Data masking is applied where production data would otherwise be exposed in development, testing or analytics. A register of the cryptographic controls in use, and of any approved exceptions, is maintained.

7.12 BUSINESS CONTINUITY AND DISASTER RECOVERY

The Organisation maintains business-continuity and restoration arrangements comprising redundant infrastructure, regular backups, defined recovery objectives and periodic restore testing, so that the integrity of the operation and the availability of critical records are preserved. Backups of critical data are taken on a regular cycle, are protected with the same controls as the production data and are held in isolated, off-site or immutable storage where feasible, and are retained in accordance with Section 11. Restore tests are performed periodically to confirm that backups can be recovered within the defined recovery-point and recovery-time objectives. Transaction-processing systems, real-time reporting and regulatory interfaces have defined fallback procedures, and the continuity arrangements are tested and reviewed at least annually and on significant change.

7.13 SECURITY GOVERNANCE AND OVERSIGHT

Executive responsibility for information-security oversight is assigned within the Organisation. Documented operating procedures are maintained for the key recurring security activities, the implementation of corrective actions is monitored, and the security policies and standards are reviewed and approved on a recurring schedule. The effectiveness of the security controls is subject to independent review, and the governance of audit and compliance data is allocated to defined owners. The Organisation operates the controls in this section as a baseline and matures them over time in line with the development of its operation and of the applicable requirements.

7.14 INCIDENT MANAGEMENT AND ESCALATION

Technical and security incidents are detected through monitoring, triaged by severity and escalated through a defined chain to the responsible technical and compliance personnel. A primary and a backup incident-response owner are designated, and roles are defined across the technical, compliance and, where relevant, legal functions; an up-to-date contact directory for internal and external escalation is maintained. Each incident is logged with its time of occurrence or confirmation, its impact, the containment and corrective actions and its resolution. Reportable incidents are reported to the CGA in accordance with Section 13, including the 24-hour incident-reporting requirement. Critical player and transaction records are hosted as described in Section 11.

8. RESPONSIBLE GAMING

This section describes how the principles of responsible gaming are implemented in the operation: the tools provided, who operates them, how at-risk behaviour is identified and responded to, and how each

interaction is recorded. It is applied together with the Organisation's Responsible Gaming Policy, which contains the controlling operational detail.

8.1 PLAYER-PROTECTION TOOLS

The Organisation provides the following tools, available at all times in the responsible-gaming section of the website or app and operable online by the player:

- Deposit limits – daily, weekly or monthly. A reduction of a limit takes effect immediately, while an increase takes effect after a 24-hour waiting period;
- Cooling-off – a short-term, player-customisable restriction from gambling, with a minimum duration of 24 hours;
- Self-exclusion – self-activated for 1, 3, 5 or 10 years or for life. The player can initiate and complete self-exclusion fully online; the selected option is enabled within 24 hours and, once effective, is irrevocable until expiry, with reactivation at expiry initiated by the player;
- Session timer – a reality-check indicator visible while the player is logged in;
- Self-assessment – a responsible-gaming self-assessment tool and information enabling the player to recognise problematic behaviour.

A fixed-period exclusion is for at least twelve months and is irrevocable during the selected period. Each election of a tool, and the time at which it takes effect, is recorded in the player account management system. The Organisation does not use responsible-gaming measures as a pretext to prevent or delay legitimate withdrawals.

8.2 VULNERABLE PERSONS

The Organisation maintains a policy to prevent vulnerable persons from playing, comprising general information on gambling addiction, procedures for identifying signs of harm, measures to prevent excessive play, and self-exclusion. Players are directed to recognised support organisations and to a self-assessment test, and may contact the Organisation's support team for assistance. The identification of a vulnerable person and any resulting action are recorded with the player account.

8.3 BEHAVIOUR MONITORING AND INTERVENTION

The Organisation actively monitors for signs of problematic gambling and applies a structured, documented response process. No single factor is treated as determinative; a determination may require multiple indicators occurring together and consistently. Monitoring is undertaken by trained frontline staff and may be supported by platform features and automated tools. Key monitoring factors include:

- sudden or unexplained increases in deposit or wagering frequency, or changes in session patterns;
- repeated failed transactions due to insufficient funds;
- repeated cancellation or reversal of withdrawal requests;
- frequent changes to responsible-gaming tools or repeated use of cooling-off;

- unreasonably increased contact with support, including agitated requests for bonuses;
- indications of a player exhausting a payment instrument; and
- attempts to open multiple accounts to bypass deposit or loss limits.

The Organisation maintains player profiles and applies a risk-based approach to the level of monitoring and intervention. All responsible-gaming interactions, whether initiated by the player or the Organisation, are recorded in the player account management system together with the indicators of concern and the actions taken. Where at-risk behaviour is identified, the player is informed of the available tools, and the Organisation follows a clear escalation protocol that may include mandatory deposit limits, temporary suspension pending assessment, or permanent exclusion in cases of severe or persistent risk. Communications on responsible-gaming matters are conducted by a person where the matter is sensitive or complex.

8.4 ADVERTISING, MARKETING AND BONUSES

Marketing, advertising and bonus activity does not encourage excessive play, is not misleading and does not target minors or vulnerable persons. Promotional terms are presented clearly and consistently with the Terms and Conditions. Players may exclude themselves from marketing, and an election to self-exclude from participation also ends the receipt of gambling marketing for the period of exclusion. Bonus mechanics are not used to circumvent the player-protection tools. Responsibility for the review and approval of marketing and bonus terms is allocated to a named function, and approved terms are recorded.

9. TERMS AND CONDITIONS

The Organisation publishes its General Terms and Conditions, which govern its relationship with players and form an integral part of the operation.

9.1 AVAILABILITY AND FORM

The Terms and Conditions are available to the player at all times, are unambiguous, and are written clearly in English and, where the target market's language is not English, also in that language. They are available for consultation from any page of the publicly accessible interface, and the version in force is the most recent text published there. The most recent text of the General Terms and Conditions in force is reproduced as Annex B to this manual and forms part of it. Each published version is recorded with its effective date, and superseded versions are retained for the period in Section 11.

9.2 MANDATORY CONTENTS

The Terms and Conditions contain at least provisions on the amendment of the terms; the name, business address and company number of the licence holder; the obligations of the player before opening an account; the conditions under which an account is closed or suspended; the conditions under which the

distribution of player funds and winnings may be suspended, cancelled or declared invalid; the currency for stakes and prize money; the retention period of communications relating to participation; the responsible gaming policy, including deposit limits and self-exclusion; withdrawal requests and the handling of dormant accounts and balances; the applicability of Curaçao law and the jurisdiction of the Curaçao courts; and a complaints procedure and ADR.

9.3 GOVERNING LAW AND CONSISTENCY

The gaming agreement is subject to Curaçao law, and disputes relating to it are brought before the Curaçao courts. Players are given a clear opportunity to review changes to the Terms and Conditions and decide whether to continue playing, with their attention drawn to changes upon login. The Organisation maintains consistency between the Terms and Conditions and this manual, in particular as to the self-exclusion durations and the fully-online self-exclusion route in Section 8, the currency and payout rules in Section 2, and the complaints and ADR process in Section 10; the review cycle in Section 1 is the control by which that consistency is preserved.

10. PLAYER COMPLAINTS AND DISPUTE RESOLUTION

This section describes how the Organisation settles disputes with players, and gives effect to the CGA Player Complaints Policy Guidelines and the Organisation's Dispute Resolution Policy.

10.1 INTERNAL COMPLAINT HANDLING

A player may submit a complaint free of charge within six months of the relevant event or bet settlement. The Organisation acknowledges receipt in writing within one week – within two days for responsible-gaming complaints, which are prioritised – and explains how the complaint will be handled. A final written determination is issued within four weeks of receipt, extendable once, in writing, by a further four weeks.

A complaint must state the player's name, address and place of residence, the account number where applicable, the date of the complaint and of the disputed event, and a description of the matter complained of, and may be submitted in any of the official languages, namely English, Dutch or Papiamentu. The Organisation makes available an official Complaint Submission Form, as a downloadable document and as an online form, in English and in the language of the website the player is using; the complaint counts in the reports under Section 13 are based on complaints submitted through this form. Each complaint is logged on receipt with its date, the player, the subject matter and the handler, and the file is updated through to outcome.

For responsible-gaming complaints the Organisation uses best efforts to resolve the matter within five business days; where more time is needed the player is informed and the resolution period does not exceed a further two weeks, extendable by a further two weeks where the delay is caused by a slow or absent response from the player. Where artificial intelligence is used in complaint handling, communications on responsible-gaming complaints and on complex complaints are conducted by a

person and not by artificial intelligence. The Organisation keeps a record of all complaints, their handling and outcome for the retention period in Section 11.

10.2 ALTERNATIVE DISPUTE RESOLUTION

Where a complaint is not resolved internally to the player's satisfaction, the player may refer it to independent alternative dispute resolution at the Organisation's expense, and is informed of this right and of how to exercise it on conclusion of the internal procedure. The ADR arrangements available to players, and the independent providers engaged, are set out in the Organisation's Dispute Resolution Policy, which forms part of the Terms and Conditions; the Organisation conforms its arrangement to any certified-provider list the CGA publishes once that list is in force.

10.3 ROLE OF THE CGA

The CGA does not determine individual complaints and does not overturn the decisions of the Organisation or an ADR provider unless a complaint has been handled inadequately. Players may contact the CGA in respect of malpractice, breaches of licence conditions or whistleblowing. The Organisation cooperates with the CGA in any review of complaint handling and submits the complaint and ADR reports in accordance with the CGA's instructions.

11. RECORDS OF CRITICAL PLAYER DATA

This section describes the digital records kept of critical information about players, their gaming transactions and their financial transactions, which are kept available to the CGA at all times.

11.1 RECORDS KEPT

The Organisation keeps digital records of critical information about players, their gaming transactions and their financial transactions, and keeps these available to the CGA. The records include player verification files, gaming-transaction records and financial-transaction records, and identify, for each transaction, the amount and nature of the credit or debit to the gaming account and, where applicable, the payment instrument used, so that any transaction can be traced back to the player and reconstructed.

11.2 HOSTING AND CGA ACCESS

The Organisation keeps these critical records on a server hosted in a Tier-IV certified data centre registered in Curaçao, and ensures that the records remain accessible to the CGA at all times, in the form and within the time the CGA specifies. The hosting arrangement, the data-centre's Tier-IV certification and the means of CGA access are documented and evidenced, the hosting invoice and certification are made available to the CGA on request, and the arrangement is kept current. Any change of hosting provider or data centre is treated as a material change under Section 1 and is notified to the CGA where

notification or prior approval is required. Where the CGA issues transitional guidance or publishes a register of approved data centres, the Organisation conforms its hosting arrangement to that guidance.

11.3 RETENTION AND INTEGRITY

Critical records are retained for at least five years, or longer where required by law, and are protected against loss or alteration through the backup and security arrangements in Sections 4 and 7, including isolated and, where feasible, immutable backup storage and periodic restore testing. Access is restricted, logged and auditable, and log integrity is protected. The CGA may request the records at any time, and the Organisation provides them in the form and within the time the CGA specifies.

12. STAFF TRAINING

This section records the permanent education provided to persons working in the field of games of chance with the Organisation.

12.1 CURRICULUM AND FREQUENCY

Persons working in the gaming operation receive permanent education annually, differentiated by role to reflect the knowledge and experience expected in that role. The training covers mental well-being, anti-bribery, crime prevention, responsible gaming, anti-money laundering, communication with players and responsible advertising. It also covers information-security awareness appropriate to the role, including the recognition of social-engineering and phishing attempts, sound authentication and credential practices, secure handling of player and financial data, and how to recognise and report a suspected incident. Frontline staff receive additional training on recognising and responding to the responsible-gaming indicators in Section 8, and compliance personnel receive training appropriate to their financial-crime responsibilities.

12.2 DELIVERY AND RECORD-KEEPING

Training is delivered by appropriate methods and conducted by the AML Officer or qualified contractors. New joiners in relevant roles receive induction training before or promptly after taking up duties, and refresher training is provided at least annually and on material regulatory or threat change. Attendance and completion are recorded and retained for the period in Section 11, so that the Organisation can demonstrate the manner and degree of its compliance with the training obligation.

13. REPORTING TO THE CGA

This section describes the reporting the Organisation provides to the CGA, the timing of each report and the function responsible for it.

13.1 REPORTS PROVIDED

The Organisation provides the CGA with all information and reports it considers necessary for monitoring compliance. The reports include at least:

- a change report covering amendments to the operation;
- an incident report;
- a player transaction report, a complaints report and an ADR report;
- a report by an independent expert approved by the CGA assessing compliance with the unusual-transaction and identification obligations; and
- a report by an independent expert approved by the CGA assessing compliance regarding system design and responsible gambling.

Responsibility for compiling and submitting each report is allocated to a named function under the oversight of the AML Officer/MLRO, and each submission is recorded with its date and content.

13.2 TIMING

The incident report is submitted within 24 hours of the incident; where reasonable assessment is required to establish whether an incident has occurred, the period begins when the incident is confirmed through investigation, save that for change and incident matters the 24-hour period is always taken to begin when the incident occurs. The complaint and ADR reports are submitted in accordance with the CGA's instructions, and the biannual amendment reports follow the 15 June and 15 January cycle.

13.3 INSPECTION

The manual and the underlying records are made available for CGA inspection within five working days of a request. The Organisation cooperates fully with the CGA's monitoring and provides updated inventories of gaming equipment, the gambling interface, application software and games offered on request.

14. AML/CFT AND SANCTIONS COMPLIANCE

This section records how the operation's financial-crime controls are organised, without reproducing internal methodology.

The Organisation's anti-money-laundering, counter-terrorist-financing, counter-proliferation-financing and sanctions controls are governed by its AML/CFT and Sanctions Compliance Policy. Customer due diligence and enhanced due diligence, player acceptance and risk classification, transaction monitoring, sanctions and politically-exposed-person screening, the identification and internal escalation of unusual transactions, reporting to the Financial Intelligence Unit, record-keeping and the related thresholds, criteria and reporting triggers are established and applied under that policy and are not reproduced in this manual or in any player-facing material.

Responsibility for the financial-crime framework rests with the AML Officer/MLRO, who also serves as the compliance officer for unusual-transaction and identification purposes and monitors compliance with the

applicable gaming law. The Organisation maintains policies and procedures at all times regarding, at least, customer identification and verification, player account and fund management, responsible gaming, information security, financial-crime compliance, and the suspension and closure of player accounts, and submits these to the CGA on request. In communications with players, such measures are described only as being applied in accordance with the Organisation's internal compliance policies and procedures.

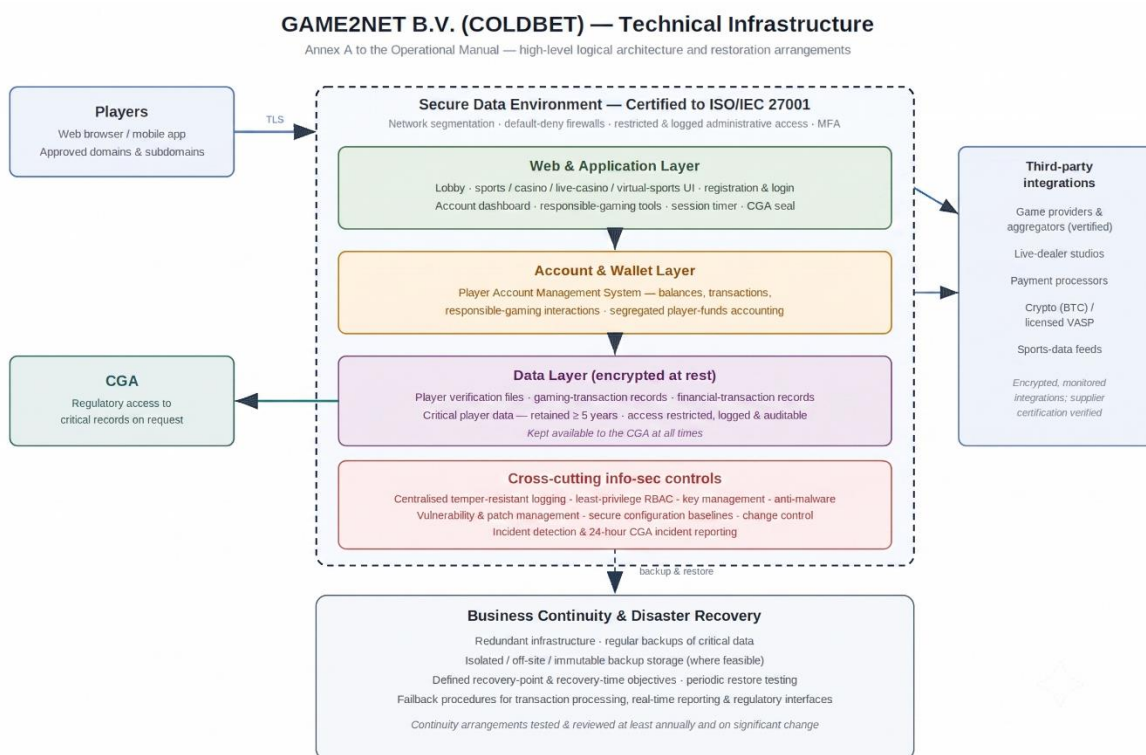
Reviewed and approved by the Director:

Mr. Dmytro Rodionov



SCHEDULE A – TECHNICAL INFRASTRUCTURE DIAGRAM

The following diagram is the high-level logical diagram of the Organisation's technical infrastructure referred to in Section 7, and gives effect to Article 5.9(1)(f) of the LOK. It shows the player-facing web and application layer, the account and wallet layer (the player account management system), the data layer holding player, gaming-transaction and financial-transaction records, the third-party integrations, the information-security controls, the Tier-IV data-centre boundary registered in Curaçao, CGA access to critical records, and the business-continuity and restoration arrangements. The Organisation keeps this diagram current and replaces it with its exact production topology on any material change to the infrastructure or hosting arrangement.



Reviewed and approved by the Director:

Mr. Dmytro Rodionov