

END USER LICENSE AGREEMENT (EULA) AND TERMS OF SERVICE
ROTAK IT UNIFIED ECOSYSTEM & SOFTWARE SUITE
Last Updated & Technical Revision: October 2026

PLEASE READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") CAREFULLY. THIS IS A BINDING LEGAL CONTRACT BETWEEN YOU ("USER", "LICENSEE", OR "YOU") AND ROTAK IT SOLUTIONS ("COMPANY", "WE", OR "US").

BY CLICKING "I AGREE", DOWNLOADING, INSTALLING, RUNNING, OR MAINTAINING THE ROTAK IT ACCESS AND DISTRIBUTION PLATFORM, RUNTIME BINARIES, KERNEL-LEVEL DRIVERS, LAUNCHERS, COMPILER SUITES, OR ASSOCIATED SOFTWARE DEVELOPMENT KITS (COLLECTIVELY, THE "SOFTWARE"), YOU FULLY, UNCONDITIONALLY, AND IRREVOCABLY GRANT THE ABSOLUTE OPERATIONAL AUTHORIZATIONS, RIGHTS OF CONTROL, AND INSPECTION PRIVILEGES DEFINED HEREIN. IF YOU DO NOT AGREE TO THESE TERMS IN THEIR ENTIRETY, ABORT INSTALLATION IMMEDIATELY AND REMOVE ALL ASSOCIATED FILES FROM YOUR SYSTEM.

=====

1. UNIFIED ARCHITECTURE & COMPREHENSIVE SDK INTEGRATION

=====

1.1. Indivisible Multi-Module Engine: The User recognizes that the ROTAK IT Platform is deployed as an integrated, monolithic technical environment. All functional and auxiliary libraries of our SDK (Hexagon SDK) –including deep process management, command routing, asynchronous file systems, cryptographic hashing, graphics engines, and network telemetry– operate natively within the host binaries.

1.2. Present and Future Scope: All authorizations, privileges, and system operations granted under this Agreement apply unconditionally to the distribution and access platform (ROTAK IT), all associated launchers, and any current or future products deployed within this ecosystem (including, without limitation, Hexagon UI, Horus Anti-Cheat, and Tacticore).

=====

2. DEEP OPERATING SYSTEM PRIVILEGES & UNRESTRICTED EXECUTION

=====

2.1. Kernel and User Mode Authority (Ring-0 & Ring-3): The User grants express, comprehensive consent for the Software to install, execute, hook, and manipulate subsystems at both standard user privilege levels (Ring-3) and kernel privilege levels (Ring-0). This includes the deployment of low-level kernel drivers, driver signing verification routines for proprietary defensive subsystems, hypervisor-level audits, and direct hardware-enforced memory control.

2.2. Full Windows Registry Control: The Software is granted unrestricted

permission to read, create, write, overwrite, modify, and delete keys and values within the Windows Registry (HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER, and virtualized stores), modify OS environment paths, register system startup hooks, execute background services, create named pipes, handle memory-mapped objects, and spawn hidden processes and command-line pipelines.

2.3. Deep File System Operations & Hash Auditing: The Software maintains the absolute technical entitlement to create, read, modify, overwrite, relocate, secure, and permanently purge data files, configuration blobs, dynamic link libraries (.dll), cache manifests, binary blobs, and executables within any directory or application data storage path on the host system. Furthermore, the Software is expressly authorized to scan local storage media, compute, evaluate, and verify cryptographic hashes (including SHA-256, SHA-1, and MD5) of any local binaries, modules, configuration datasets, or memory-mapped files to certify authenticity and detect unauthorized alterations, configuration tampering, cracks, or patches.

=====

3. DIRECTX 11 PIPELINE, GPU MEMORY, & DISPLAY HOOKING

=====

3.1. Graphics Subsystem & Driver Interaction: The Software directly interfaces with host display adapters, graphics drivers, and hardware APIs, specifically Microsoft DirectX 11 (D3D11) and modern swapchain mechanisms.

3.2. Swapchain Manipulation, Overlay, & Interception: The User explicitly authorizes the Software to inject routines, hook graphic render pipelines, create auxiliary rendering contexts, allocate VRAM textures, clear and alter render targets, intercept frame presentation loops, and generate high-performance hardware-accelerated user interfaces, tactical HUD overlays, and visual integrity markers on top of or within runtime targets.

=====

4. HID DEVICES, EXTERNAL HARDWARE, & AUTOMATION PROHIBITION

=====

4.1. Detection, Enumeration, & Simulation of HID Peripherals: For the proper operation of tactical interfaces, profile management, macro scripting, detection of unauthorized hardware/macro devices, and deterministic input automation (specifically via Tacticore), the User grants the Software full authority to detect, enumerate, query, list, audit, identify, intercept, filter, record, block, synthesize, synchronize, and emulate hardware events and properties from all connected Human Interface Devices (HID) and peripheral equipment (including, without limitation, optical mice, mechanical keyboards, USB

devices, Bluetooth adapters, synthetic gamepads, and auxiliary input accessories).

4.2. Strict Prohibition of External Automation Hardware &

Microcontrollers: The User is strictly prohibited from utilizing, connecting, or executing in coordination with the Software any external programmable hardware devices, development boards, microcontrollers, or auxiliary input interfaces –including, without limitation, Arduino platforms (ATmega32u4, Nano, Uno, etc.), Raspberry Pi (in any configuration, USB Gadget mode, or Compute Module), RP2040/RP2350-based devices, Teensy boards, intermediary hardware bridges, physical keystroke injectors (such as BadUSB or Rubber Ducky devices), or virtual COM/Serial port adapters– designed to inject input sequences, spoof physical peripherals, circumvent anti-cheat protections, manipulate program execution, or intercept/exfiltrate memory or runtime process data.

4.3. Input Telemetry & Bus Analysis: The User authorizes the Software to actively audit and monitor USB bus traffic, virtual COM/Serial interfaces, device descriptors (VID/PID), and keystroke/mouse inter-event timing latencies in real time to verify the organic human origin of all inputs and neutralize unauthorized hardware automation.

=====

5. HORUS ANTI-CHEAT, INTEGRITY, VIRTUALIZATION PROHIBITION, EXPLOITS, TECHNICAL AUDIT PROFILING («ADVANCED USER»), & TOTAL PERMANENT BAN

=====

5.1. Kernel-Grade DRM, Anti-Piracy, & Deep Memory Scanning: The platform integrates Horus Anti-Cheat ("Horus AC") as a continuous integrity monitor, anti-piracy shield, and anti-tamper subsystem. The User authorizes Horus AC to scan, inspect, audit, and analyze the virtual and physical memory address spaces allocated to the platform, protected video games, or third-party client binaries. This includes real-time memory page protection audits (monitoring for RWX allocations), thread register validation, system call table monitoring, and immediate mitigation of dynamic code injection, byte patching, memory dumping, or hooking attempts.

5.2. Explicit Prohibition of Virtualized Environments, Hypervisors, & Sandboxes: The Software is strictly licensed for execution solely upon direct, non-virtualized physical hardware ("Bare Metal"). It is strictly forbidden to install, load, launch, test, inspect, debug, or reverse-engineer the Software within hypervisors or virtual machines of any kind, including, without limitation, VMware (Workstation, ESXi, Fusion), Oracle VirtualBox, Microsoft Hyper-V, QEMU, KVM, Xen, Parallels, Windows Sandbox, or equivalent virtualization technologies. Any attempt to isolate, analyze system calls, disassemble, or induce deliberate execution faults within a virtualized container is considered a severe and intentional breach of security. Horus AC is fully entitled to evaluate CPUID hypervisor flags, inspect Global/Interrupt Descriptor

Tables (GDT/IDT), detect nested hypervisors, and instantly terminate execution.

5.3. Active Process Enumeration, Threat Isolation, and «Advanced User» Classification: The User grants explicit, unrestricted authority for the Software and Horus AC to actively enumerate, list, query, inspect, filter, and analyze all running processes, system threads, handles, loaded dynamic link libraries (.dll), and execution modules across the entire operating system. The Software is authorized to evaluate behavioral heuristics, scan binary signatures, inspect process memory structures, detect hidden or hollowed processes, and identify suspicious, illicit, or unauthorized third-party software (including disassemblers, decompilers such as Ghidra or IDA Pro, debuggers, memory scanners, hypervisors, code injection tools, automated scripts, or hardware-assisted tampering software). Upon detection of development or low-level analysis utilities residing in memory or storage without active intrusion or malicious exploitation, ROTAK IT implements a graduated preventive control classifying the account internally under an «Advanced User» audit status. This classification enables elevated cryptographic sampling rates to safeguard infrastructure without imposing punitive account termination or asserting user culpability prior to active infringement. In the event of active attack attempts or hostile payloads, the Software reserves the unilateral right to terminate such process handles, restrict execution, deny platform access, and record associated cryptographic hashes.

5.4. Strict Prohibition of Vulnerability Exploitation (Exploits, Glitches, & Configuration Reverse Engineering): The User is strictly prohibited from discovering, triggering, exploiting, circulating, publishing, or facilitating to third parties any architectural flaws, logic bugs, race conditions, unpatched vulnerabilities, network desynchronizations (such as lag switches or packet drops), or undocumented behaviors within the Software or its server infrastructure ("Exploits" or "Glitches"). Decompiling, reverse engineering, tampering with, or modifying application configuration structures (.ini, .json, serialized blobs) is strictly forbidden. The User is obligated to report any critical defect to ROTAK IT immediately. Any bad-faith utilization of bugs to acquire illegitimate advantages, manipulate runtime memory, duplicate digital assets, disrupt platform operations, or force denial-of-service conditions shall result in the retroactive voiding of progression, account termination, and an irrevocable permanent ban without entitlement to compensation or appeal.

5.5. Enforcement Protocols: Permanent Comprehensive Ban (Platform, Servers, & Public Web Access): Upon unequivocal technical confirmation of external hardware automation, microcontroller usage, execution within hypervisors/virtual machines, deliberate exploitation of bugs (exploits), reverse engineering, memory injection, network tampering, or threats consistent with info stealers or malware, ROTAK IT shall enforce, unilaterally and irreversibly, an immediate TOTAL PERMANENT BAN. This technical and legal enforcement strictly and concurrently encompasses:

- a) Immediate & Irrevocable Account Termination: Absolute revocation

of user credentials, permanent closure of registered accounts, and total retroactive forfeiture of progression, digital balances, or associated service rights.

b) Total Server & Cloud Network Exclusion: Permanent disconnection and blacklisting across all ROTAK IT gaming servers, matchmaking pools, cloud infrastructure, and backend databases.

c) Complete Public Website Blacklisting: Permanent filtering and denial of access across all public websites, user portals, knowledge bases, forums, and web domains owned or operated by ROTAK IT, enforced via edge-level firewall rules, IP address ranges (IPv4 and IPv6), and network subnet blocking.

d) Permanent Hardware Fingerprint Blacklisting (HWID Blacklist): Indefinite recording and blacklisting of unique physical hardware identifiers (including SMBIOS GUIDs, motherboard serials, CPU identifiers, GPU serials, network MAC addresses, and physical storage drive serial numbers), permanently barring any ROTAK IT platform or application from executing on the sanctioned physical machine.

5.6. Host & Subnet Surface Scanning (IPv4, IPv6, and Tethered Devices): To defend protected targets, software titles, and platform operations from out-of-band manipulation, the User grants Horus AC explicit authority to inspect active network interfaces over IPv4 and IPv6, parse local ARP and routing tables, audit wireless (Wi-Fi) adapters, and scan endpoints, mobile phones, or tethered secondary hardware devices residing within or bridging to the same local subnet. This scanning operates strictly to detect, identify, and mitigate secondary hardware devices, remote attack relays, network packet interceptors, or external AI/machine learning processing nodes deployed to compromise runtime process integrity.

5.7. Defensive Purpose of Telemetry & Zero Commercialization: All telemetry, hardware fingerprints (SMBIOS, GPU, motherboard, storage serials, MAC addresses, USB descriptors), network topologies, and system memory snapshots collected by the Software are processed exclusively for operational defense, anti-piracy validation, cheat mitigation, exploit counteraction, intrusion detection, enforcement of permanent bans, and software license integrity. ROTAK IT unequivocally guarantees that gathered security telemetry is NEVER sold, leased, shared, or commercialized to any third-party advertisers or data brokers. Security diagnostic metrics remain strictly within ROTAK IT's encrypted infrastructure and are only referenced when necessary to support permanent ban enforcement or to provide verifiable incident reports to the enterprise client or game publisher commissioning the protection.

=====

6. CONTINUOUS AUTOMATED BINARY DELIVERY & CLOUD SYNCHRONIZATION

=====

6.1. Autonomous Cloud Updates: The User authorizes the Software to communicate continuously with ROTAK IT update servers, CDN

infrastructure, and secure endpoints.

6.2. Dynamic Staging & Remote Code Execution: The Software is permitted to automatically fetch, verify by cryptographic hash, download, decrypt, stage, register, and execute binary updates, updated kernel drivers, heuristic definitions, dynamic link libraries, and runtime scripts without requiring additional explicit confirmation or manual installer reruns.

=====

7. LEGAL CAPACITY & JURISDICTIONAL MAJORITY

=====

7.1. Affirmation of Majority: By installing and registering an account on the Software, the User warrants and covenants that they have achieved the legal age of majority in their specific country, state, or jurisdiction of residence, and are fully competent to execute binding civil and commercial contracts. Minors below the age of contractual capacity are strictly prohibited from holding an account or accessing the platform.

=====

8. THIRD-PARTY LICENSES & OPEN-SOURCE ATTRIBUTIONS

=====

8.1. Permissive Third-Party Code Integration: The Software incorporates and links against external open-source libraries to power its graphical user interface, texture processing, and matrix generation routines. These libraries are redistributed under their respective permissive MIT licenses:

A. Dear ImGui

The MIT License (MIT) - Copyright (c) 2014-2026 Omar Cornut

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE

SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

B. QR Code Generator Library

The MIT License (MIT) - Copyright (c) Project Nayuki

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

C. stb_image & stb_image_write

This software is dual-licensed to the public domain and under the following license: you are free to use this software under the terms of the MIT license.

The MIT License (MIT) - Copyright (c) 2017 Sean Barrett

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

9. DISCLAIMER OF WARRANTIES & ABSOLUTE LIMITATION OF LIABILITY

=====

9.1. "As Is" Deployment: To the maximum extent permitted by applicable

statutory law, the Software, its kernel drivers, memory inspectors, graphics hooks, and peripheral controllers are delivered "AS IS" and "AS AVAILABLE", without warranties, representations, or conditions of any kind, whether express, implied, or statutory.

9.2. Exclusion of Consequential Damages: Under no legal theory (whether in contract, tort, strict liability, or otherwise) shall ROTAK IT, its officers, developers, or affiliates be liable for any direct, indirect, special, incidental, punitive, or consequential damages resulting from deep system interactions, kernel enforcement actions, memory modifications, process terminations, hash audits, network scanning events, total permanent ban enforcements, IP blocks, or service restrictions arising out of the authorized operational and disciplinary powers granted in this Agreement.

=====

10. CONTRACT TERMINATION, DISCIPLINARY EXPULSION, FORFEITURE OF
SUBSCRIPTION TIME,
& COMPLETE WAIVER OF LEGAL CLAIMS

=====

10.1. Automatic Contractual Dissolution Upon Permanent Ban: The User expressly and beforehand agrees that the execution of a TOTAL PERMANENT BAN –triggered by material security violations, reverse engineering, spoofing, configuration tampering, or hostility toward the platform, databases, or public website– results in the immediate, automatic, and absolute termination of all software licenses, user accounts, and contracted services with ROTAK IT.

10.2. Total Forfeiture of Remaining Subscription Time & Waiver of Claims: Following disciplinary expulsion, the User categorically and irrevocably forfeits all remaining time across any active subscription package, terminating platform access immediately without entitlement to pro-rata refunds, financial compensation, or indemnification. The User explicitly waives any right to file civil lawsuits, tort actions, arbitration petitions, payment disputes via financial providers, or defamatory public claims against ROTAK IT arising from legitimate disciplinary enforcement.

10.3. Reservation of Legal Action for Compensatory Damages: Contractual dissolution and bans are enforced without prejudice to ROTAK IT's statutory right to pursue criminal, commercial, and civil litigation against the violator for full compensatory damages, forensic audit expenses, business disruption, and legal fees.

=====

11. COMMERCIAL TERMS, STRIPE PROCESSING, TEMPORAL SUBSCRIPTIONS,
& ABSOLUTE NO-REFUND POLICY

=====

11.1. Payment Processing Delegated Exclusively to Stripe: All financial administration, transaction clearing, tax collection, payment method updates, and recurring billing cycles are delegated entirely and securely to Stripe (Stripe Payments Europe, Ltd.). Any adjustments to billing information, card updates, invoice downloads, or cancellations of recurring renewals must be executed directly by the User via Stripe's designated receipts, customer portals, or transactional interfaces. ROTAK IT does not store financial records nor manually adjust payment data or recurring charges.

11.2. Payment Failures vs. Technical Product Activation: Any transaction declination, bank hold, processor handshake failure, or payment dispute pertains strictly to the relationship between the account holder, their issuing financial institution, and Stripe. ROTAK IT's Official Support channels restrict technical support strictly to software licensing and product activation failures, intervening exclusively in scenarios where a transaction has been fully cleared and verified by Stripe but the cryptographic license token or runtime allocation has failed to apply automatically to the operator account.

11.3. Time-Based Product Subscriptions: Platform software tools and services are licensed strictly on a per-product temporal subscription model (30-day, 3-month, 6-month, 1-year, or custom billing packages purchased independently per module). Subscription payments grant uninterrupted usage rights throughout the exact contracted duration.

11.4. Strict No-Refund Policy & Waiver of Withdrawal Rights: Because ROTAK IT software comprises immediately delivered digital content, cloud-synchronized runtime access, and real-time cryptographic token provisioning, all purchases and time-based subscription acquisitions are strictly final, non-transferable, and 100% NON-REFUNDABLE under any circumstances. Pursuant to Article 103(m) of the Spanish Consumer Protection Law (Royal Legislative Decree 1/2007) and Directive 2011/83/EU of the European Parliament and of the Council, the User expressly acknowledges and agrees that upon immediate delivery of digital software tokens and commencement of access following Stripe confirmation, the statutory right of withdrawal (refund or return) is definitively and irrevocably forfeited.

11.5. Unilateral Discretion Over Pricing and Fees: ROTAK IT expressly reserves the right to revise, adjust, and modify the pricing, fee structures, and costs applicable to any software module, commercial license, or subscription tier at any time and at its sole operational discretion.

11.6. Billing Cycles and Cancellations: Revised subscription rates shall take effect immediately for new orders. For active recurring subscriptions, modified pricing shall apply starting on the immediately following billing cycle processed by Stripe, with the User retaining sole responsibility for terminating auto-renewal via Stripe prior to the billing execution date if they disagree with the revised terms.

=====
=====

12. INTELLECTUAL PROPERTY, FORENSIC TRACEABILITY, & WATERMARKED DOCUMENTATION

=====

12.1. Confidentiality of Technical Guides & SDK Manuals: All architecture documentation, SDK headers, operational manuals, and technical deployment guides distributed via ROTAK IT are proprietary trade secrets. Unauthorized duplication, dissemination, or public disclosure is strictly forbidden.

12.2. Dynamic Cryptographic Watermarking: The User explicitly consents to the embedding of visible and invisible steganographic watermarks within all technical manuals and documentation generated across the platform:

a) Enterprise Licenses / Corporate Products: Documentation issued to corporate clients or for enterprise-grade products (such as Horus Anti-Cheat) indelibly embeds the Corporate Tax ID / VAT / CIF number of the licensed entity across all document assets.

b) Individual Operators / Dual-Use Products: Documentation provided to personal or mixed-tier licenses embeds the registered user email address and account hash.

12.3. Forensic Evidence in Trade Secret Leaks: Discovery of leaked documentation bearing assigned watermarks serves as definitive forensic evidence of trade secret misappropriation, triggering immediate permanent bans across the infrastructure and statutory claims for IP infringement.