AVIS Land
Cybercrime Prevention and Incident Response Statement

Version 1.0 | 25 November 2026

This Statement establishes the cybersecurity, incident-response and cooperation requirements for GENESIS operations on AVIS Land and its QUANTUM gateway. It governs safeguarding across marketplace, financial, research, manufacturing and other connected services according to each operator's actual role, authority and applicable law.

1 Issuing operators and contact

The issuing operators are GENESIS Collateral House Company Limited, Irish company number 823931, registered at 51 Bracken Road, Dublin D18 CV48, Ireland, and GENESIS Collateral House Company, North Carolina entity number 3214399, registered at 4111-E Rose Lake Drive, Charlotte, North Carolina 28217, USA. GENESIS operates within the Monkeyrock group. Each operator remains accountable for the activities it undertakes.

Security reports and enquiries: legalcube@avis.land. Telephone and WhatsApp: +34 674 002 006. Principal operating and correspondence office: GENESIS, 17–25 Via Ingegno, 84087 Sarno (SA), Italy. Website: https://avis.land. These channels receive initial reports; sensitive evidence shall move through an appropriately secured channel agreed with the responsible incident team.

2 Connected services and independent responsibilities

AVIS Land connects public users, independent vendors, franchisees, subsidiaries, system providers, researchers, universities and industrial participants as a technology cluster. GENESIS shall protect the systems it operates and coordinate relevant interfaces. Each participant remains responsible for its own systems, personnel and services, subject to its agreements and legal duties. Financial institutions, issuers, custodians, manufacturers and insurers retain their distinct responsibilities.

Users retain ownership of their assets and rights. Operational access permits only the safeguarding, processing and support authorised by the applicable service and lawful mandate. Incident response does not authorise unrelated exploitation, unrestricted disclosure, appropriation or disposal of user assets. GENESIS shall identify the affected operator, provider, data role and asset custodian before exercising powers. Outsourcing a task does not discharge the operator's own obligations.

3 Governance preparation and accountability

Each operator's governing body shall approve the security programme, resource material risks and receive incident and remediation reporting. Management shall designate an accountable security lead, incident commander and deputies, with escalation to legal, privacy, financial-crime, operational-safety and communications functions. Provider responsibilities and emergency decision authority shall be documented before relevant services operate.

GENESIS shall maintain inventories of critical services, systems, data, assets, privileged identities and dependencies, with owners and impact-based priorities. Response plans shall address disruption, integrity loss, unauthorised access and fraud, including insider misuse, ransomware, denial-of-service attacks and combined cyber and physical events. Contact routes, alternative communications, recovery objectives and decision records shall support continued response when ordinary systems

are unavailable. Training and exercises shall be proportionate to risk, with actions assigned and tracked to closure.

4 Identity access and separation of duties

Access shall require an attributable identity, appropriate verification and the minimum authority needed for the task. Privileged and remote access, financial administration and other high-risk functions shall use multifactor authentication, with phishing-resistant methods where appropriate. Shared credentials shall be avoided; exceptional shared access requires controlled assignment and traceability. Service accounts and robotic identities shall have constrained permissions, accountable owners and managed lifecycles.

Approvals, payment execution, changes to sensitive records and independent reconciliation shall be separated according to risk. Access shall be reviewed periodically and promptly changed when duties, contracts or employment end. Emergency privileges require recorded justification, time limits and subsequent review. Credential recovery must verify the requester through an appropriate independent process; convenience or seniority does not justify bypassing a required safeguard.

5 Payment diversion impersonation and account takeover

Instructions involving new beneficiaries, changed bank or wallet details, unusual withdrawals, corporate actions or sensitive account recovery shall receive checks proportionate to value, novelty and risk. Changes must be authenticated through a trusted route independent of the message requesting them. Contact details supplied in a suspicious message must not become the verification source. Material changes and high-risk transfers shall receive independent approval where required by the assessed risk.

Staff shall assess business-email compromise, forged invoices, compromised supplier accounts, deepfake voice or video, urgency and impersonation. Familiar wording, a recognisable voice or a successful login alone is insufficient proof of authority. Suspected takeover requires prompt review of sessions, credentials, recovery details, recent instructions and connected identities. Any temporary restriction shall be proportionate, recorded and reviewed.

6 Secure development patching and vulnerability reports

Software and infrastructure changes shall follow controlled development, review, testing and release processes. Risk assessments shall address dependencies, exposed services, configuration, tenant separation and data flows. Vulnerabilities shall be prioritised by exploitability, impact and exposure; urgent risks require prompt correction or documented compensating protection. Production changes require appropriate approval, rollback arrangements and checks that essential functions remain intact.

Security researchers may report suspected vulnerabilities through the contact channel. Testing requires express authorisation defining systems, methods, timing, data handling and stop conditions; submitting a report does not grant wider access. Researchers must avoid disruption, unnecessary access, persistence and disclosure of personal information. GENESIS shall assess good-faith reports without retaliation for the report itself, coordinate correction and agree appropriate disclosure. No participant may hack back or access another party's systems without lawful authority.

7 Secrets cryptographic assets and recovery material

Passwords, private keys, recovery phrases, signing credentials, tokens and other secrets shall be protected according to their sensitivity and use. Controls shall govern creation, custody, access, rotation, backup, recovery and revocation, with stronger isolation or hardware protection where justified by risk or law. Secrets must not be embedded in public code, ordinary support messages or unrestricted logs. Signing authority and recovery authority shall be separately controlled where appropriate.

Suspected compromise requires assessment of affected permissions and transactions, controlled revocation or rotation, and preservation of evidence. Rotation must account for dependent services and continuity. Backups shall be protected from unauthorised alteration and production compromise; restoration shall be tested according to service criticality. A recovery process must not expose a user's assets to a person who lacks authority over them.

8 QUANTUM robotic and automated systems

QUANTUM connections, APIs, robotic team members and automated agents shall operate within explicit service permissions and transaction mandates. Untrusted documents, messages, retrieved content, model output and inter-agent instructions shall not override access rules. Tool permissions, network access, data retrieval and financial or physical actions shall be constrained outside the model's instructions. Material commitments require the approval specified for that activity.

Controls shall address prompt injection, poisoned datasets, malicious dependencies, model manipulation and unintended disclosure between participants. Data provenance, changes and relevant outputs shall be recorded proportionately. Material automation changes require controlled evaluation, staged introduction, monitoring and a workable rollback or safe-stop procedure. Human review shall be available for significant exceptions. Automation must not independently widen its authority, suppress an incident report or approve its own sensitive access.

9 Industrial systems physical safety and connected production

Manufacturing, construction, laboratories, waste-to-nanopowder and graphene processing, materials handling and robotic equipment require security decisions coordinated with qualified operational and safety personnel. Remote access and connections between business and industrial systems shall be controlled according to risk. Critical operating settings, engineering files and safety-related changes require authorised review and traceability.

Containment shall consider personnel, hazardous materials, equipment condition and process stability. Responders must not disable safety interlocks or abruptly stop a process without assessing the physical consequences. Safe operating or shutdown procedures shall take priority where life or health is threatened. Recovery requires appropriate verification of process settings, equipment integrity and safe conditions, as well as technical restoration. Cyber response must cooperate with site emergency arrangements.

10 Third parties cloud services and supply chains

Providers shall be assessed according to the access, data and critical functions entrusted to them. Agreements shall establish security responsibilities, timely incident cooperation, relevant subcontractor controls, continuity, evidence availability, secure exit and lawful audit or assurance rights proportionate to the service. Required regulatory access rights shall be preserved. Provider notification arrangements must allow the operator to meet its own deadlines.

GENESIS shall assess concentration and dependency risks, including common cloud services, software components and administrators. Supplier access shall be limited and withdrawn when no longer required. A provider incident shall be assessed for its effect on each affected service and legal entity. A provider's assurances or insurance do not replace GENESIS's responsibility for its own decisions and controls.

11 Privacy children and restricted information

Security monitoring and investigations shall use a lawful basis, necessary data and proportionate access. Personal information shall be protected in collection, transfer, analysis and retention, including international transfers. Investigation access shall be limited to authorised personnel; unrelated participant information must not be circulated through the technology cluster. Retention

shall follow applicable schedules and justified preservation holds, with secure disposal when retention is no longer required.

Tower 27 and other services involving children require particular attention to account safety, safeguarding, age-appropriate communications and the consequences of disclosure. Reports must avoid exposing a child's identity unnecessarily. Suspected exploitation or imminent danger shall be escalated through appropriate safeguarding and competent-authority routes. Staff shall not copy or redistribute unlawful abusive material; preservation and reporting must follow lawful specialist procedures.

12 Monitoring and reliable records

GENESIS shall maintain monitoring appropriate to critical services and material threats, including unusual access, privilege changes, payment diversion, data extraction, destructive activity and unauthorised robotic actions. Detection coverage, alert handling and escalation shall have accountable owners. Relevant records shall identify the actor or machine, time, affected system, action, approval and outcome without unnecessarily capturing secrets or personal data.

Time sources shall be sufficiently consistent for investigation, and important logs protected against unauthorised alteration and deletion. Monitoring access itself shall be controlled. Investigators shall distinguish evidence, inference and unresolved questions; an alert is not proof of wrongdoing. Security-sensitive configurations, detection details and exploitable information shall be shared only with authorised recipients who need them.

13 Reporting an incident and protecting victims

Users and personnel should report suspected fraud, compromise, unsafe robotic behaviour, data exposure or suspicious instructions promptly to legalcube@avis.land or +34 674 002 006. Include the affected service, approximate time, description and safe contact details. Never send passwords, authentication codes, private keys or recovery phrases. Avoid opening suspicious attachments again or forwarding malicious files through ordinary support channels. Where physical danger is imminent, contact local emergency services immediately.

For a suspected unauthorised payment, promptly contact the bank, payment provider or custodian through independently verified details and request available protective or recovery measures. Preserve transaction references and relevant communications. Cryptocurrency reports should preserve available transaction hashes and addresses without exposing keys. Recovery is not assured; demands for further payments to unlock supposedly recovered funds require independent verification. Good-faith reporters and victims shall receive respectful treatment without retaliation for reporting.

14 Triage containment and evidence preservation

The incident lead shall record receipt, establish severity and affected scope, activate relevant specialists and assign decision owners. Assessment shall consider service interruption, data and asset integrity, losses, personal information, children, physical safety and cross-border effects. Discovery, legal awareness, classification and materiality decisions shall be separately timestamped and reassessed as facts develop. Escalation must not reset a statutory clock.

Containment may include isolating affected systems, restricting sessions, disabling compromised credentials, pausing suspect instructions and contacting relevant custodians. Measures must be lawful, necessary and proportionate, preserving safe unaffected services where practicable. Before destructive changes, responders shall preserve relevant logs, messages, transaction records, snapshots and volatile evidence where feasible without compromising safety. Evidence records shall identify collection method, time, custodian, integrity checks such as hashes, transfers and access. Working copies shall be separated from preserved originals where practicable.

15 Funds ransomware and response authority

Suspected diverted funds shall be referred rapidly to the responsible bank, payment provider, exchange or custodian for lawful recall, restriction or preservation. GENESIS shall act only within its authority and shall not seize unrelated user assets. Financial-crime specialists shall assess linked fraud, sanctions and suspicious-activity obligations. Communications with suspected offenders shall be controlled by the incident lead and legal function.

Ransom or extortion payments are not automatically authorised. Any proposal requires executive approval, legal and sanctions assessment, consideration of recovery alternatives, applicable reporting and licensing requirements, and relevant law-enforcement and insurance arrangements. An insurer's agreement does not override law. No staff member or automated agent may independently commit to payment. Payment does not establish that systems will be restored, information deleted or further demands prevented.

16 Legal notification decisions and personal data breaches

The responsible legal and compliance functions shall maintain an entity- and territory-specific reporting matrix identifying each trigger, authority, deadline, responsible owner, filing route and required follow-up. Relevant customer and provider duties shall be included. Decisions, supporting facts, lawful exceptions and submissions shall be recorded. Initial reports shall use available facts and be supplemented when necessary; investigation must not postpone a required notification.

Where GDPR applies, a controller shall notify the competent supervisory authority without undue delay and, where feasible, within 72 hours after awareness of a personal-data breach, unless it is unlikely to risk individuals' rights and freedoms. Reasons for delay must accompany late notification. A processor shall notify its controller without undue delay. Where high risk is likely, affected individuals shall be informed without undue delay unless a lawful Article 34 exception applies. All personal-data breaches and reporting decisions shall be documented.

17 Financial sector and national reporting obligations

An entity within DORA's scope shall classify and report major ICT incidents under the applicable rules, including incidents originating at providers. Under Regulation 2025/301, initial notification is required as early as possible, within four hours of major classification and ordinarily within 24 hours of awareness. If classification occurs after those 24 hours, notification is due within four hours of classification. Intermediate reporting is due within 72 hours of initial notification, with required updates; final reporting is due within one month of the intermediate or latest updated intermediate report. Any applicable exception or inability to meet a deadline shall be handled as the regulation requires.

NIS obligations shall be assessed under the national legislation currently applicable to the entity and service, including relevant NIS2 implementing measures. U.S. state breach laws and sector rules require separate assessment. For a reporting issuer subject to Form 8-K Item 1.05, a material cyber incident must generally be disclosed within four business days after materiality is determined; that determination must occur without unreasonable delay after discovery. Lawful exceptions require documented review.

18 Cooperation confidentiality and financial crime reporting

GENESIS shall cooperate with competent regulators, police, CSIRTs and other authorised bodies through verified channels and an applicable legal basis. Requests shall be assessed for authority, scope and required response. Disclosures shall be limited to what is lawful and necessary, preserving confidentiality, applicable privilege and evidence integrity. Lawful preservation requirements shall be communicated to relevant custodians and providers.

The designated financial-crime function and locally required money-laundering reporting officer shall assess relevant suspicions under the AML programme and submit reports when required. A police or cyber report does not replace an independent financial-intelligence reporting duty. Communications must respect suspicious-report confidentiality and tipping-off restrictions. Participants may receive appropriate updates and assistance where lawful without disclosure that compromises an investigation or exposes another person's protected information.

19 Recovery communications and continuous improvement

Restoration shall follow documented priorities and verified recovery criteria, addressing the entry route, persistence, compromised credentials and affected data. Systems shall be checked before reconnection, with reconciliation of relevant payments, balances, transactions and production records. The responsible owners shall approve return to service and monitor for recurrence. Safety-critical operations require the relevant operational approval.

Affected parties shall receive accurate, proportionate information about relevant impact, protective steps and available contact routes, subject to lawful restrictions. Confirmed facts shall be distinguished from estimates; unsupported attribution and premature claims of complete recovery shall be avoided. After stabilisation, management shall review causes, response effectiveness, losses, control gaps and reporting performance, assign corrective actions and validate completion. Findings shall inform training, supplier management, design and continuity arrangements.

20 Insurance oversight and continuing obligations

Insurance arrangements, including participation by a group insurance business, shall be assessed against the actual policy, insured entity, covered event, limits, exclusions, conditions and claims process. The incident team shall preserve relevant evidence and meet applicable notice and cooperation requirements. Availability of a policy or insurance relationship does not guarantee cover, payment, restitution or recovery and does not replace legal notifications or protective action.

Management shall review this Statement at least annually and after material incidents, legal changes or changes in services. NIST CSF 2.0 and SP 800-61 Revision 3 shall inform the security and incident-management programme, with relevant official guidance adapted to the operation. Assurance statements must be supported by evidence and their stated scope. This Statement preserves mandatory rights, legal reporting obligations and the specific responsibilities of each operator and provider.

Reference publications

NIST Cybersecurity Framework 2.0

NIST SP 800 61 Revision 3 Incident Response Recommendations 2025

NIST SP 800 82 Revision 3 Guide to Operational Technology Security

Ireland Data Protection Commission personal data breach notification guidance

DORA Regulation EU 2022/2554

Commission Delegated Regulation EU 2025/301 on major ICT incident reporting

SEC cybersecurity risk management governance and incident disclosure compliance guide

OFAC updated ransomware sanctions advisory 2021