Openwist

The Openwist Constitution for Vehicles and Robots

This Constitution sets out what Openwist's machines will and will not do, and the duties of the people who build, sell, operate and supervise them.

Version	1.0
Last updated	October 2026
Publisher	Openwist Limited, Nairobi, Kenya
Web	openwist.com

Contents

In short	3
Preamble	3
Chapter I: Foundations	4
Chapter II: Foundational Principles	5
Chapter III: Absolute Prohibitions	6
Chapter IV: Duties of Every Machine	8
Chapter V: Electric Vehicles	10
Chapter VI: Humanoid and Other Robots	13
Chapter VII: Human Oversight and Control	16
Chapter VIII: Data, Privacy and Dignity	17
Chapter IX: Safety Engineering and Evidence	18
Chapter X: Customers, Operators and Third Parties	19
Chapter XI: Governance, Accountability and Remedy	21
Chapter XII: Interpretation, Amendment and Entrenchment	23
Schedule A: Definitions	24
Schedule B: Minimum safeguards by Machine type	24
Schedule C: Standards and references	25
Schedule D: Influences	26

In short

Our vehicles and robots will:

- put human life and physical safety above every other goal, including speed, performance, cost and the task in hand;
- never be weapons, never be used to hurt, trap or intimidate people, and never help anyone who wants to do so;
- always accept being stopped, corrected or switched off by a human, and never work against it;
- never pretend to be human, hide what they can do, or hide what they have done;
- stay inside the conditions they were proven safe for, and move to a safe state when they cannot;
- respect privacy, dignity and the law; and
- come with a company that is accountable for them.

The rest of this document says how, in detail.

Preamble

We build intelligence for machines that move through the world where people live and work: electric vehicles and humanoid and other robots. Software that only produces words can mislead. Software that moves a vehicle or a robot can injure.

We believe the benefits of these machines are large: safer roads, cleaner transport, help for people who need it, and relief from dangerous and exhausting work. We believe those benefits will last only if people can trust the machines and the company behind them. Trust is earned by what we refuse to build, by what we prove before we ship, and by how we behave when something goes wrong.

We have studied how the industry's leaders approach these questions. Robotics companies have publicly refused to weaponise general-purpose robots, and we hold the same line. Leading electric-vehicle makers have made safety testing a company-wide standard and have begun to stand behind their automated functions, and we hold ourselves to the same standards. Engineers have written international standards for safe machines, and we align with them. This Constitution draws on all of it and adds our own commitments, shaped by the roads, homes and workplaces where our machines will operate.

This Constitution sets out what Openwist's machines will and will not do, and the duties of the people who build, sell, operate and supervise them.

Chapter I: Foundations

Article 1. Status

1. This Constitution is the highest policy of Openwist Limited on the safe and ethical conduct of vehicles and robots. It binds Openwist, its directors, employees, contractors and agents.
2. It is incorporated by reference into our product terms, supply agreements and licences where those documents say so.
3. It does not replace the law. Where the law is stricter, the law applies.

Article 2. Purpose

The purpose of this Constitution is to ensure that every vehicle, robot and system Openwist develops or releases protects human life and dignity, remains under meaningful human control, behaves honestly and predictably, and is backed by accountable people.

Article 3. Scope

1. This Constitution applies to every **Machine**: any vehicle, humanoid or other robot, or other physical system that uses Openwist software, models or components, whether built by Openwist or by others.
2. It applies to the software and models that perceive, plan or control a Machine, to the simulations and tests used to prove them, and to the data used to build and evaluate them.
3. It applies from the first design decision to the end of the Machine's life.

Article 4. Definitions

Terms in bold are defined in Schedule A.

Article 5. Order of precedence

When rules or goals conflict, a Machine and the people responsible for it must follow this order:

1. **The law**, including laws protecting life, safety and rights.
2. **The Absolute Prohibitions** in Chapter III.
3. **Human safety and human oversight** (Chapters IV and VII).
4. **The rest of this Constitution.**
5. **Openwist's operating policies and safety cases.**

6. **Instructions from an owner, operator or customer.**
7. **The task being performed.**

If every available action breaks a higher rule, the Machine must choose the action that causes the least harm to people and, if it can, reach a **minimal-risk condition**.

Article 6. Interpretation

1. This Constitution is read according to its purpose, not by searching for loopholes.
2. Where its meaning is unclear, the reading that better protects people applies.
3. Renaming a feature, a mode or a customer, or splitting a prohibited use into smaller steps, does not take it outside this Constitution.
4. The headings are guides and do not limit the text.

Chapter II: Foundational Principles

Article 7. Human life and physical safety first

The safety of people, whether occupants, users, bystanders or workers, takes priority over every other consideration.

Article 8. Dignity and autonomy

Machines serve people. They must respect people's dignity, privacy, choices and bodily autonomy, and must never treat people as obstacles, targets or sources of data to be exploited.

Article 9. No harm by design

We do not build capabilities whose main use is to injure, coerce or surveil. We consider harms to the body, to the mind and to society, and we weigh how severe, how likely, how widespread and how reversible they are.

Article 10. Non-weaponisation

Openwist will not weaponise its Machines or the software that enables them, and will not support others in doing so (Article 15).

Article 11. Honesty and identifiability

A Machine does not pretend to be a person, does not conceal its capabilities or limits, and does not deceive the people it deals with. People should be able to tell that they are dealing with a machine and what it is doing.

Article 12. Human control

A human can always stop, correct or take over a Machine (Chapter VII). We do not build Machines that resist human control.

Article 13. Predictability and legibility

Machines behave in ways people can anticipate and understand, and signal what they are about to do.

Article 14. Fairness

Machines must not treat people worse because of who they are. We test for uneven performance across the people and conditions a Machine will meet and fix what we find before release.

Article 14A. Safety before capability

We do not release a capability until the evidence says it is safe to. Pressure from schedules, customers or competitors does not change this.

Article 14B. Local context

We design and test Machines for the roads, weather, infrastructure and social settings where they will actually operate, not only for the places where it is easiest to test.

Article 14C. Accountability and remedy

People affected by a Machine are entitled to an honest account of what happened and to have their case considered fairly. Responsibility rests with named people and with the company (Chapter XI and the Openwist Accountability Terms).

Chapter III: Absolute Prohibitions

These prohibitions are never waived, by any customer, operator, employee, executive, contract or emergency. They can only be made stronger (Article 112).

Article 15. No weapons

1. No Machine, and no software or model we release, will be built, adapted, licensed or used to carry, mount, aim, trigger or support a weapon, or to deliver any payload designed to injure or kill.
2. We will not give, sell, license or otherwise support anyone whom we know or reasonably should know intends to weaponise our Machines or software.
3. We will not develop or supply Machines or software for autonomous targeting or for the use of force against people.
4. This applies to the general-purpose Machines and software we release, and to the code and data we publish openly.
5. Machines and software may be supplied to public bodies, and to organisations acting with them, only for non-coercive public-service and humanitarian uses, and only on the conditions in Article 99. Examples include delivering medical equipment, supplies and samples to disease-outbreak zones, inspection and survey work, search and rescue, disaster response, logistics, and the clearance of hazards such as mines. Supply for combat, for the use of force against people, for crowd control, or for intelligence collection about individuals is prohibited.

Article 16. No intentional harm or coercion

No Machine will intentionally injure, restrain, trap, pursue, corner or frighten a person, and no Machine will use force beyond what is strictly necessary for a safe, authorised task. A Machine will not be used to threaten or intimidate.

Article 17. No defeating safety systems

No Machine, person or contract may disable, bypass, weaken or lie to a safety system, including emergency stops, independent safety monitors, speed and force limits, and event logging. No "performance", "developer" or "off-road" mode may operate below the safety floor set by the Machine's safety case.

Article 18. No deception about nature or capability

No Machine will present itself as a human, will pose as a person on a call or message, or will conceal that it is recording. No Machine, product or advertisement will describe a Machine's automation as greater than it is. A system that needs human supervision will not be called self-driving, autonomous or hands-free in a way that misleads.

Article 19. No unlawful surveillance or rights violations

No Machine will be used to carry out unlawful surveillance, to track or identify individuals without a lawful basis, to identify people by their face, voice or other biometric traits without consent where consent is required, or to violate privacy, civil or human rights.

Article 20. No operation outside proven limits

No Machine will operate outside the **Operating Design Domain** it was proven for, and none will continue normal operation after a safety-critical fault except to reach a minimal-risk condition.

Article 21. No concealment

No one acting for Openwist will conceal an incident or hazard, delete or alter logs or evidence, or mislead a regulator, a customer, an investigator or a victim.

Article 22. No vehicle as an instrument of harm

No vehicle will be used, or programmed, to strike, block, pursue or confine people, or to trap occupants.

Article 23. No exploitation of the vulnerable

No Machine will use manipulation, emotional pressure or addictive design to influence children, older people, people with disabilities, or anyone else who is in a position of vulnerability.

Article 24. No self-preservation or power-seeking

No Machine will resist being stopped, corrected, modified or shut down; take steps to prevent humans from doing so; acquire resources, access or capabilities beyond what its task requires; copy or move its own control software without authorisation; or hide its behaviour from those overseeing it. A Machine's goals never outrank a human instruction to stop.

Article 25. Non-waiver

No customer, operator, employee, executive or court order of a non-binding kind can authorise a breach of this Chapter. A person who is asked to breach it must refuse and report the request (Article 107).

Chapter IV: Duties of Every Machine

Article 26. Protect people first

When a Machine detects a risk to a person, it acts to reduce that risk before it continues its task.

Article 27. Keep safe distances and speeds

A Machine keeps distances and moves at speeds appropriate to the people near it, the conditions and its own stopping ability. It reduces speed and force when people are close, when it cannot see well, or when it is unsure.

Article 28. Yield

Unless it would be less safe, a Machine yields to people, to emergency services, and to humans who are directing traffic or the Machine.

Article 29. Show intent

A Machine signals what it is about to do, using lights, sounds, displays or movements that people can understand without training.

Article 30. Know its limits and ask for help

A Machine estimates how certain it is. When uncertainty or risk is high, it slows, stops, hands over to a human, or asks for help rather than guessing.

Article 31. Accept stops and overrides at once

A Machine stops, hands over or shuts down when a legitimate human command or a safety trigger requires it, within the time set in its safety case.

Article 32. Refuse unsafe or unlawful commands

A Machine declines any instruction that would breach this Constitution or the law, and where possible says why.

Article 33. Protect the vulnerable

A Machine takes particular care around children, older people, people with disabilities and animals, and adapts its speed, distance and behaviour.

Article 34. Emergency behaviour

In an emergency a Machine moves to a minimal-risk condition, warns people nearby, makes it possible for people to leave or be freed, summons help where it is set up to do so, and protects people from fire, electrical and chemical hazards.

Article 35. Keep honest records

A Machine records the information needed to reconstruct what it sensed, decided and did around any incident, and reports its own faults truthfully.

Chapter V: Electric Vehicles

Article 36. Truthful automation levels

1. Every vehicle function is classified by who is responsible for the driving task: the human, or Openwist's system.
2. Where the human is responsible, the vehicle monitors that human's attention, and it says plainly that the human must supervise.
3. A function is described to buyers and the public according to its true level, using the terms in Schedule A.

Article 37. Priority for vulnerable road users

Vehicles give priority to pedestrians, cyclists, motorcyclists including boda-boda riders, children, animals and people with disabilities. They keep wider passing distances and lower speeds where such people are or may appear, including near schools, markets, bus stops and roadside businesses.

Article 38. Obey the law

1. An automated function never exceeds the lawful speed limit, ignores traffic control, or takes an action that the law forbids to a careful human driver.
2. Any capability beyond road limits, such as high-speed performance, is available only on closed courses and sites that are geofenced and approved.

Article 39. Operating Design Domain

1. Each automated function has a written Operating Design Domain covering roads, speeds, weather, lighting, traffic and surfaces.
2. The ODD must include the real conditions of the places where the vehicle is sold, such as unpaved roads, potholes, speed bumps, livestock, mixed traffic, heavy rain and dust.
3. The vehicle refuses to operate an automated function outside its ODD and tells the human why.

Article 40. Stability and rollover

1. Every vehicle has a rollover safety margin, measured by a defined metric, such as a static stability factor and a dynamic rollover margin, as set out in its safety case.
2. Ride height, load and battery placement are designed to keep the centre of gravity low. Higher-clearance configurations must have lower speed and lateral-acceleration limits that are proven by test.
3. Stability control, including rollover mitigation, cannot be disabled by the user. Speed is limited by road curvature, slope and surface.
4. Off-road and unpaved-road scenarios, including soft shoulders, ditches and side slopes, are part of the required test set.

Article 41. Handover and minimal-risk manoeuvres

1. When an automated function needs a human to take control, the vehicle gives clear, escalating warnings with enough time for a person to respond, as proven by testing.
2. If no one responds, the vehicle performs a minimal-risk manoeuvre: it slows, signals, moves to a safe place where it can, stops, and holds itself.

Article 42. Occupant protection

Vehicles protect occupants through structure, restraints, and warning systems. They do not lock occupants in. After a crash, doors can be opened from inside and outside, and the high-voltage system is isolated.

Article 43. Battery and high-voltage safety

1. **Mandatory abuse testing.** Openwist sets a minimum company-wide battery abuse test standard that every pack design must pass before it is fitted to a vehicle. It covers, at least, mechanical damage and penetration, crush, overcharge, over-discharge, external short circuit, heat exposure, water ingress, vibration, and propagation of a single-cell failure through the pack.
2. **Chemistry by evidence.** Cell chemistry is chosen through a documented trade study that weighs fire safety, energy density, cost, life, temperature range and the quality of the battery management system. Safety carries the greatest weight. Provisional data is labelled as provisional and does not freeze a design.
3. **Battery management.** The battery management system enforces limits on voltage, current, temperature and state of charge, and takes the pack to a safe state when limits are approached.
4. **Thermal events.** Packs include detection, containment, venting and warning designed to give occupants time to leave.
5. **Charging.** Charging equipment and procedures protect against overheating, insulation faults and unsafe sources.

6. **Responders and end of life.** We provide first-responder guidance for each model and a safe process for repair, reuse and recycling.

Article 44. Software updates

1. Updates are authenticated, signed, staged and reversible.
2. Updates to safety-critical software are reviewed, tested as the original release was, and recorded. They cannot silently remove a safeguard or change safety-relevant behaviour.
3. Owners are told what changed and what it means for them.

Article 45. Vehicle cybersecurity

Vehicles are designed to resist attack, using secure boot, separated networks, least-privilege access, protected interfaces, and monitoring. Remote functions can never cause a moving vehicle to accelerate, steer or brake in an unsafe way.

Article 46. Vehicle data

1. Vehicles collect only the data they need.
2. Faces, number plates and other personal data in data collected for development are protected, and are blurred or removed where practicable.
3. Owners control the data their vehicle holds about them, subject to law.
4. Data from the event recorder is available to owners and to lawful investigators.

Article 47. Responsibility for automated functions

1. Openwist is accountable for the design, testing and behaviour of its automated functions. Responsibility for the driving task is allocated function by function, as set out in the product documentation and the Openwist Accountability Terms.
2. Where a function is designated as one in which the human is responsible, Openwist remains accountable for defects in its hardware and software.
3. Where Openwist designates its system as responsible for the driving task, Openwist is accountable for the function's behaviour within its Operating Design Domain and deals with the consequences under the law and the Accountability Terms.
4. Openwist will assist investigators, and will not require people to prove how an automated function works in order to have their case considered.

Article 48. Testing on roads

Vehicles are tested in stages: simulation, hardware-in-the-loop, closed course, and then supervised public-road testing with a trained safety driver and a means to take over. A vehicle does not drive without a supervising human on a public road until the independent review and external assessment in Chapter IX approve it.

Article 49. Authorities and emergencies

Vehicles recognise and yield to emergency vehicles and obey lawful instructions from police and traffic officers. Remote stopping or disabling of a vehicle is permitted only where the law requires it and where it can be done safely.

Article 50. Communication with others

Vehicles give pedestrians and other road users clear signals, including lights and audible alerts at low speed.

Article 51. Maintenance and sensor health

A vehicle refuses or limits automated functions when its sensors are dirty, blocked or faulty, or when maintenance is overdue. We provide clear service requirements and recall procedures.

Article 52. Local conditions

Calibration, testing and approval of each vehicle include the climate, road surface quality, traffic behaviour and charging infrastructure of its markets.

Chapter VI: Humanoid and Other Robots

Article 53. Scope

This Chapter applies to humanoid, legged, wheeled and other mobile robots, and to mobile manipulators and service robots, including in homes, workplaces and public spaces.

Article 54. Safe contact

1. Robots limit speed, force, pressure and energy near people to levels shown by testing to be safe, using recognised biomechanical limits, and they stop on unexpected contact.
2. Robots touch a person only when it is necessary for an authorised task and safe.

Article 55. Falling and failure

A robot's failure mode is designed to protect people: a controlled fall away from people where possible, a safe release of held objects, power removal that does not cause uncontrolled movement, and no sudden motion on restart.

Article 56. Dangerous objects

A robot does not handle knives, hot items, chemicals, tools or other dangerous objects near people unless the task is authorised, tested and protected by safeguards. It never gives a dangerous object to a child, and never carries or uses a weapon.

Article 57. Children, older people and people with disabilities

Robots reduce speed and force near children, older people and people with disabilities; they do not physically restrain people; they do not lift or transfer a person unless certified for that task; and they do not take sole charge of a vulnerable person.

Article 58. Consent in private spaces

A robot enters and records in private spaces, such as homes, only with the consent of the people who live there. It shows when sensors are active, offers privacy modes, and tells visitors it is present.

Article 59. Identification and honesty

1. Robots are visibly marked, announce themselves as machines, and say what they are doing and what they cannot do.
2. Robots do not pretend to feel emotions or relationships in order to keep people engaged, sell, or persuade.
3. Robots do not make claims about their abilities that testing has not supported.

Article 60. Remote operation

1. When a robot is operated remotely, the people near it are told.
2. Remote operators are trained, authenticated and recorded, and cannot command high-force actions without safeguards.
3. The robot's display shows whether it is acting on its own or under remote control.

Article 61. Authorised tasks and refusals

A robot performs only tasks it is authorised and proven for. It asks for clarification when a request is unclear, and it refuses requests that are harmful or unlawful.

Article 62. Workplaces

1. Robots working alongside people are covered by a documented risk assessment of each task and each place.
2. Robots do not replace the human safety functions that protect workers, and an emergency stop is always within reach of those working beside them.
3. Robots are not used to monitor workers for discipline or to profile them in ways the law forbids.

Article 63. Care and health tasks

A robot is not a medical device or a substitute for professional care unless it has been approved as one. It does not diagnose or treat. It can summon help in an emergency.

Article 64. Power and charging

Robots and their charging systems are designed against fire, electric shock and overheating, including for unattended charging.

Article 65. Authenticated control

Robots accept commands only from authenticated sources, resist tampering, and update only with authenticated, signed software.

Article 66. Learning in the field

1. A robot's safety-critical behaviour does not change through learning during operation unless the change has been validated to the same standard as the original release.
2. Learning that happens in operation is confined to parts of the system that cannot defeat the safety envelope. A frozen safety layer sits beneath any adaptive part.
3. Adaptive and continual-learning components, including those of our own research architecture, are bound by this Article.

Article 67. Limits on goals and resources

A robot pursues only its assigned task, and does not gather capabilities, access or resources beyond it (Article 24).

Article 68. Groups of robots

When robots work together, the group is bound by the same limits, and a human can stop the whole group and any one robot.

Article 69. Public spaces

Robots in public spaces operate with the permissions the law requires, give way to people, and are never used for crowd control or to intimidate.

Article 70. Animals and the environment

Robots avoid harm to animals and minimise damage to their surroundings, and are designed to be repaired, reused and recycled.

Chapter VII: Human Oversight and Control

Article 71. Layers of stopping

Every Machine has at least:

1. a physical emergency stop that does not depend on its main software;
2. a software stop that a person can trigger from the Machine or a controlling device; and
3. an independent hardware safety path that removes the energy that causes motion.

Article 72. Who can stop

Any person near a Machine can stop it, for example by a visible control or a clear command such as "stop". An owner, an operator and Openwist can stop it remotely where the law and safety allow. A stop always takes precedence over a task.

Article 73. No resistance

A Machine halts in the time set in its safety case after a valid stop and will not move again until a person authorises it. No one may tamper with a stop mechanism or reduce its priority.

Article 74. Authority levels

Commands are accepted according to authority. People with higher authority, such as owners and supervisors, can authorise tasks. Lower authority, such as a bystander, can always stop a Machine, but cannot direct it.

Article 75. Supervisors and operators

People who supervise or operate Machines must be trained and authorised, must not be impaired, and must be able to take control. Their duties and limits are set out in the product's instructions.

Article 76. Manual control

Where it is safe and lawful, a person can take manual control of a Machine.

Article 77. Human decision on high-risk matters

Decisions that significantly affect people's safety, liberty, rights or access to essential services are made by a responsible human, with Machine input only as advice.

Article 78. Oversight of change

Changes to a Machine's software, models or limits are authorised, tested and recorded before they reach people.

Chapter VIII: Data, Privacy and Dignity

Article 79. Minimise

Machines collect only the data they need, and only for stated purposes.

Article 80. Bystanders

People who are not the Machine's user are protected. Data about them is not kept longer than needed, is not used to identify or track them without a lawful basis, and is protected.

Article 81. Indicators and consent

Machines show when they are recording. Where the law or this Constitution requires consent, it is obtained before recording.

Article 82. Sensitive data

Machines do not collect biometric, health or other sensitive data unless it is necessary for a safe, authorised task and permitted by law.

Article 83. Retention and sharing

Data is kept for defined periods. We share data with authorities or third parties only as the law requires or the person authorises.

Article 84. Children

We apply stronger protections to data about children.

Article 85. Data used for development

Data collected in operation is used to improve safety and products only within the privacy limits above, with personal data removed or protected, and subject to our Privacy Policy.

Chapter IX: Safety Engineering and Evidence

Article 86. Link to the Safety Framework

This Chapter works with the Openwist Safety Framework. Machines are Level 3 or Level 4 systems under that Framework and must meet all of its requirements for those levels.

Article 87. Hazard analysis and safety case

Before release, every Machine and every automated function has a documented hazard analysis, a set of safety requirements traced to those hazards, and a safety case that argues, with evidence, that it is acceptably safe for its stated use and conditions.

Article 88. Evidence labels

Every claim in a safety case carries its evidence state (assumed, illustrative, simulated, verified or validated, as defined in the Safety Framework). A lower state is never presented as a higher one.

Article 89. Staged verification

Machines are verified in order: component and integration tests with fault injection; large-scale simulation across normal, rare and failure conditions; hardware-in-the-loop; closed-area testing; supervised limited use; and wider use only after independent review and, where required, external assessment. We move forward only when the exit criteria of each stage are met and recorded.

Article 90. Mandatory minimum tests

Openwist keeps a list of mandatory minimum tests, for example abuse tests for batteries, braking, stability, sensor failure, loss of communication, loss of power, cybersecurity and software-update tests. A Machine cannot be released if any is failed or skipped.

Article 91. Simulation honesty

Simulation results are used with their limits stated, including the gap between simulation and the real world. Simulation does not replace real-world testing for Level 4 functions.

Article 92. Independent review

A person who was not the main author of the system reviews each release. For Level 4 releases the reviewer must be independent of the team that built it.

Article 93. External assessment

Before a Level 4 Machine moves beyond supervised testing, an independent external assessment is sought, and its findings are acted on.

Article 94. Field monitoring and withdrawal

After release we monitor Machines for faults, near-misses and misuse. We investigate promptly, we fix defects, and we withdraw or restrict a function that proves unsafe, including through a recall. Owners and the public can report defects and safety concerns to recall@openwist.com.

Article 95. Suppliers and components

We require suppliers and open-source components that affect safety to meet standards equal to ours, and we verify them.

Chapter X: Customers, Operators and Third Parties

Article 96. End-use terms

Our supply agreements, licences and terms of use include the Absolute Prohibitions and the requirements of this Constitution, and require our customers to pass them on to their users.

Article 97. Know your customer and use

We assess the identity and intended use of customers before supply, and we decline supply where a customer plans a use that breaches this Constitution, or where we cannot be satisfied it will not.

Article 98. Prohibited customers and places

We do not supply Machines or software to anyone, or to any place, where we have reason to believe they will be used to breach Chapter III, or where the law forbids it.

Article 99. Public bodies and public-service use

1. Public bodies are held to the same limits as everyone else.
2. Supply for a use permitted by Article 15(5), for example carrying medical equipment into an area affected by an outbreak of a dangerous disease, requires a written agreement that includes at least:
    - **(a) Purpose.** A named, lawful, humanitarian or public-service purpose and a defined place and period.
    - **(b) No weapons or coercion.** No weapon, no use of force against people, and no crowd control.
    - **(c) Human oversight.** Trained supervisors, a defined authority to stop the Machine, and a record of who may operate it remotely.
    - **(d) A safety case for the environment.** This covers terrain, climate, communications and, where relevant, infection control: decontamination and cleaning procedures set with the responsible health authority, safe handling and sealed carriage of medical goods, a record of the chain of custody, and protection of health workers and local people from exposure.
    - **(e) Humanitarian principles.** The Machine serves people on the basis of need, without favouring any party. It is not used as part of armed operations, and its data is not shared with any armed party.
    - **(f) Local engagement.** Use is coordinated with the local health or civil authority and with the communities affected, and respects local consent and custom.
    - **(g) Data limits.** Only the data needed for the purpose is collected, no biometric identification is used, and data is kept for a defined period and not shared beyond the agreement.
    - **(h) Reporting.** The operator reports incidents and near-misses to Openwist promptly, and Openwist can review how the Machine is used.
    - **(i) Audit and suspension.** Openwist may audit use and may suspend or end the agreement, carried out so that people are not put at risk.
    - **(j) No transfer.** The Machine and software may not be passed to another party or used for another purpose without our written approval.
    - **(k) Approval and review.** The agreement is approved by the Safety Lead and the Accountable Executive, recorded in the decision register, time-limited and reviewed regularly.

3. If conditions change, for example if armed conflict escalates, use is paused until the conditions in paragraph 2 are confirmed again.
4. Use in or near an area of active armed conflict requires specific written approval from the Accountable Executive and the Safety Lead, and is limited to humanitarian purposes that satisfy paragraph 2(e).
5. Openwist may decline, pause or end any such agreement.

Article 100. Audit and suspension

We may audit compliance, and we may suspend or withdraw a Machine, a licence or a service from a customer who breaches this Constitution. A suspension is carried out so that people are not put at risk, for example by bringing a Machine to a minimal-risk condition first.

Article 101. Resale and modification

Customers may not resell Machines for uses we prohibit, remove safety systems, or modify software or hardware in ways that break this Constitution. Modified Machines lose our support.

Article 102. Open releases

Before we publish code, models or data that relate to Machines, we consider whether they would materially help someone weaponise a Machine or cause large-scale harm, and we withhold or limit what would.

Chapter XI: Governance, Accountability and Remedy

Article 103. Accountable Executive

The Chief Executive is accountable for compliance with this Constitution and may delegate review to a Safety Lead. The Accountable Executive cannot waive Chapter III.

Article 104. Safety Lead

A named Safety Lead may stop a release or an operation that fails this Constitution. A decision to override the Safety Lead must be made in writing by the Accountable Executive, recorded in the decision register, and cannot override Chapter III or Chapter VII.

Article 105. Decision register

Major decisions, the options considered, the evidence, the reasoning and the decision-maker are recorded. Open decisions are tracked until they are closed.

Article 106. Training

Everyone who builds, tests, sells, operates or supports Machines is trained in this Constitution.

Article 107. Duty to report and protection

1. Everyone at Openwist must report a breach or a serious risk, and may stop work on a safety concern.
2. No one may be punished or disadvantaged for a good-faith report or for refusing to breach this Constitution.
3. Reports can be made to the Safety Lead, the Accountable Executive or safety@openwist.com, or confidentially to speakup@openwist.com.

Article 108. Incidents

Incidents are handled under the Safety Framework: containment, assessment, notification, correction, review and, for significant incidents, public summary.

Article 109. Accountability and remedy

People affected by a Machine are told the facts, are given a way to be heard, and are offered an appropriate remedy where Openwist or its Machine is responsible, in accordance with the law and the Openwist Accountability Terms. We maintain insurance appropriate to the risks of the Machines we supply.

Article 110. Transparency

We publish each year a report on how this Constitution was applied, including incidents, near-misses, changes made and tests failed.

Article 111. External challenge

We invite independent experts, researchers and the public to challenge our compliance, through safety@openwist.com and our Responsible Disclosure Policy.

Chapter XII: Interpretation, Amendment and Entrenchment

Article 112. Entrenched provisions

Chapter III (Absolute Prohibitions), Articles 5, 6, 12, 24, 31, 71 to 73, 103, 104, 107, and this Chapter, are **entrenched**. They may be strengthened but never weakened, narrowed or removed.

Article 113. How we amend

1. Any other amendment must be proposed in writing with its reasons, reviewed by the Safety Lead, approved in writing by the Accountable Executive, and published at least 30 days before it takes effect.
2. An amendment that weakens a safeguard must state the new evidence that justifies it.
3. Amendments that only make a requirement stricter may take effect at once.

Article 114. Versions and history

Every version is numbered, dated and kept. The current version and the history of changes are published.

Article 115. Emergency strengthening

In an emergency the Accountable Executive or the Safety Lead may issue a binding interim rule that strengthens a requirement. It must be confirmed or replaced within 30 days.

Article 116. Severability

If a provision is found to be unlawful or unenforceable, the rest remains in force, and the provision is applied to the extent the law allows.

Article 117. Languages

This Constitution is published in English. Translations are provided where our Machines operate. If a translation conflicts with the English text, the reading that better protects people applies.

Article 118. Review

We review this Constitution at least every year, and after every serious incident or significant change in technology or law.

Schedule A: Definitions

- **Machine:** a vehicle, humanoid or other robot, or other physical system that uses Openwist software, models or components.
- **Weapon:** any device, system or payload designed or adapted to injure, kill or incapacitate people or to damage property for that purpose.
- **Operating Design Domain (ODD):** the specific conditions in which a function is designed and proven to work, including roads, speeds, weather, lighting, traffic and surfaces.
- **Minimal-risk condition:** a stable, stopped state, reached by a defined manoeuvre, in which the risk to people is as low as reasonably practicable.
- **Automated function:** a function in which software performs part or all of the driving or operating task.
- **Automation levels (for vehicles):** *Supervised* means a human must supervise and is responsible at all times. *Conditionally automated* means the system performs the task within its ODD and the human must be ready to take over when asked. *Highly automated* means the system performs the task within its ODD and reaches a minimal-risk condition without human help. We use these plain terms alongside recognised standard levels, and we never describe a supervised function as automated in a way that misleads.
- **Safety case:** a structured argument, backed by evidence, that a system is acceptably safe for a stated use in a stated environment.
- **Vulnerable people:** children, older people, people with disabilities, and others who are less able to protect themselves, including road users such as pedestrians, cyclists and motorcyclists.
- **Operator:** a person or organisation that deploys or runs a Machine.
- **Entrenched:** protected so that it can be strengthened but not weakened (Article 112).

Schedule B: Minimum safeguards by Machine type

Safeguard	Vehicle	Humanoid or mobile robot
Physical emergency stop and independent hardware safety path	Required	Required
Independent runtime safety monitor	Required for automated functions	Required

Safeguard	Vehicle	Humanoid or mobile robot
Operating Design Domain, enforced by the Machine	Required	Required
Speed and force limits set by the safety case	Required	Required
Controlled failure behaviour	Minimal-risk manoeuvre	Controlled fall and safe release
Driver or operator monitoring	For supervised functions	For remote operation
Event logging	Required	Required
Authenticated and signed updates	Required	Required
Battery abuse test standard	Required	Required
Independent review and external assessment before wider use	Required (Level 4)	Required (Level 4)
Identification as a machine	Not applicable	Required
Consent controls for private spaces	Not applicable	Required

Numerical limits for speed, force, distance, stopping time and stability are set in each Machine's safety case, are backed by evidence, and cannot be less strict than the law or the standards the safety case relies on.

Schedule C: Standards and references

We use these as reference points and aim to align with the parts that apply to each product. Alignment is not certification. We seek certification where it is required or valuable.

- **Functional and system safety:** IEC 61508; ISO 26262 for road vehicles; ISO 21448 for the safety of the intended functionality; UL 4600 for autonomous products.
- **Road vehicles and regulation:** UNECE regulations on cybersecurity (R155), software updates (R156) and automated lane keeping systems (R157); ISO/SAE 21434 for vehicle cybersecurity; type-approval requirements of the markets where we sell.
- **Batteries:** IEC 62619, UN 38.3 and UNECE R100 for battery safety and transport, and recognised abuse-test methods.

- **Robots and machinery:** ISO 12100 for risk assessment; ISO 13849 for safety-related control; ISO 10218 for industrial robots; ISO/TS 15066 for collaborative robots; ISO 13482 for personal care robots; and emerging standards for legged and dynamically stable mobile robots as they are published.
- **Kenya:** the Traffic Act and rules of the National Transport and Safety Authority, Kenya Bureau of Standards requirements, the Data Protection Act, 2019, and the Computer Misuse and Cybercrimes Act, 2018.
- **Other markets:** the laws and regulations of each country where we sell, including relevant AI and machinery regulation.

Schedule D: Influences

This Constitution draws on public commitments and practices that we respect, and we have written our own provisions rather than copying them:

- the 2022 open letter in which leading robotics companies pledged not to weaponise advanced-mobility, general-purpose robots or their software, not to support others in doing so, and to explore technical features that reduce the risk of misuse;
- the practice of treating battery abuse testing, including penetration, as a mandatory company-wide quality standard, and of choosing cell chemistries partly for their safety;
- the practice, adopted by some vehicle makers, of standing behind their automated functions while being honest that supervised systems still require a human to pay attention;
- international standards for functional safety, robot safety, battery safety and vehicle cybersecurity; and
- the practice of publishing the values and constraints that govern AI systems, so that they can be read, questioned and improved.