Code of Conduct

Visar Systems AB | Version 1.0 | 26 November 2026

Policy owner: Simon Ekman, CEO

Approver: Board of Directors

Board approval date: 2026-11-26

Purpose and scope

We conduct business honestly, treat people with respect and take responsibility for the effects of our work. This Code sets the behaviour expected of everyone working for or representing Visar Systems AB, including employees, management, directors, consultants and advisors.

It applies in the workplace, online, at events and in dealings with customers, suppliers, partners and the open-source community. We expect business partners to respect these principles and address relevant expectations in our agreements.

Respect, dignity and fair treatment

Treat others professionally and respectfully, including when you disagree. Discrimination, harassment, sexual harassment, bullying, threats and degrading treatment are unacceptable. Employment and business decisions must be based on relevant, fair criteria.

Respect human rights, freedom of association and lawful collective bargaining. We do not accept forced labour, child labour or exploitation in our operations or business relationships. Raise concerns when a partner’s practices conflict with these principles.

A safe and sustainable working environment

Follow workplace safety instructions, report hazards and help prevent harm to physical and mental health. Respect reasonable working hours, recovery and personal boundaries. Managers must address unsafe conditions and unacceptable behaviour.

Use energy, equipment and other resources responsibly. Reduce unnecessary waste, travel and purchases where practical, reuse equipment securely and arrange responsible disposal of electronic waste. Environmental claims must be accurate and supportable.

Honest business and independent judgement

Comply with applicable law and our contractual obligations. Communicate accurately about our products, security, capabilities and commercial terms. Do not conceal material limitations, falsify records or claim certifications or approvals we do not hold.

Do not offer, request or accept bribes or improper advantages, directly or through others. Gifts and hospitality must be modest, transparent and incapable of improperly influencing a decision. Cash or cash equivalents must not be offered or accepted. If uncertain, seek management guidance before proceeding.

Disclose actual or potential conflicts of interest promptly, including personal relationships, outside work or financial interests that could affect judgement. Do not take part in a conflicted decision until it has been assessed and appropriately managed.

Compete fairly. Do not agree prices, allocate markets or exchange competitively sensitive information improperly with competitors. Select suppliers and partners on relevant business, quality, security and ethical grounds.

Protect information, assets and intellectual property

Protect customer information, personal data, confidential business information and company assets. Access and use information only for authorised purposes and follow its classification and handling requirements. Confidentiality obligations continue when a role or engagement ends.

Respect copyright, software licences and the intellectual property of others. Follow applicable open-source licence and attribution requirements. Use company systems and AI only within approved policies; do not bypass controls or disclose information through unapproved services.

Responsible technology and customer relationships

For civilian, defence and dual-use applications, consider foreseeable misuse and harm when designing products, accepting work and supporting customers. Raise concerns about intended use, security or human-rights impacts before proceeding. Observe applicable restrictions on trade, sanctions and export, and obtain appropriate advice when requirements are unclear.

Do not access a customer environment, collect customer data or expand a support activity without the required authorisation. Report security concerns promptly through the appropriate security process.

Speak up and handle concerns fairly

Raise suspected misconduct promptly with the CEO. You may instead contact the Chair of the Board if the concern involves the CEO or you are uncomfortable reporting to the CEO. You do not need conclusive proof to raise a concern honestly.

We will assess reports fairly, involve only those who need to know and protect personal data. Confidentiality will be respected as far as possible, but absolute secrecy cannot be promised where an investigation or legal duty requires disclosure. A person with a conflict must not lead the handling of that report.

Retaliation against anyone who raises a concern honestly or assists an investigation is prohibited. Deliberately false allegations are unacceptable. Reporting here does not prevent anyone from using applicable external reporting channels or contacting a competent authority.

Responsibilities and review

This Code applies to everyone working for or representing Visar. Managers must lead by example. Those covered by the Code must seek guidance when unsure and cooperate with appropriate investigations.

Breaches may lead to corrective action, restrictions on access or changes to an employment or business relationship, subject to applicable law and agreements. The response must be fair and proportionate.

Management will review this Code at planned intervals, according to an internally documented schedule, and when significant changes occur. The approved version and reporting routes must be communicated to the people covered by it.