AEO Programme: Don’ts

DONT’S: The AEO Programme participants are expected not to:

Compliance & Continuous Readiness

(i) Do not consider the AEO status as one time compliance fulfillment, since the AEO status is contingent on continued compliance.

(ii) Do not ignore any suspension proceedings without remedial actions. Failure to have the suspension withdrawn is a revocation ground.

(iii) Do not reapply during the ineligibility window after revocation.

(iv) Do not miss the self-declaration window, where applicable. Auto-renewal is conditional on self-declaration and its review.

(v) Do not claim MSME relaxations without a valid MSME certificate.

(vi) Do not assume physical non-verification means records need not be audit-ready. OSPCA and the three-year review still apply.

(vii) Do not allow the eligibility or security criteria on the basis of which AEO status was granted to lapse during the validity of the certificate.

(viii) Do not submit a self-declaration or compliance declaration without undertaking an appropriate internal verification of the facts and supporting records.

(ix) Do not assume that the availability of AEO facilitation dispenses with the requirement to comply with the underlying Customs, GST or other applicable laws.

Communication & Disclosure

(x) Do not wait beyond 14 days to report a significant change.

(xi) Do not continue to use the AEO certificate after a change of legal entity. A new legal entity needs to apply afresh.

(xii) Do not suppress a Customs error. Undisclosed errors, or errors with no remedial action, count against the holder.

(xiii) Do not ignore communications from the AEO Cell, Programme Manager or designated CRM relating to compliance, review, suspension, renewal or other AEO matters.

Supply Chain Security & Business Partners

(xiv) Do not use an uncertified or unreviewed business partner for a security-sensitive leg.

(xv) Do not allow gaps in supply-chain security controls, including controls relating to personnel, premises, cargo, conveyance, business partners and IT systems.

(xvi) Do not engage or continue with a business partner in a security-sensitive activity without carrying out the prescribed/appropriate due diligence.