

Guidelines for security incident reporting

In accordance with subsection 6 (1) of Regulation of the Government of the Republic of Estonia No. 39 of 24.03.2016 “Procedure for Provision and Receipt of Security Information of Ports, Port Facilities and Ships”, the Estonian Transport Administration as the competent authority for maritime security and the focal point gives the following instructions:

- (1) **Bomb threats.** If a bomb threat is considered credible, and action such as search or evacuation is initiated, the Estonian Transport Administration must be notified immediately. In the case of a bomb threat that is not considered credible, immediate notification is not required. A full record of each incident shall be retained for possible future evaluation.
- (2) **Incidents of which the media are aware.** If the media become aware, or are believed to be aware, of an incident or occurrence, it is important that the Estonian Transport Administration be notified immediately.
- (3) **Discovery of explosives.** Discovery of explosives on board of a ship or port facility must be reported to the Estonian Transport Administration immediately.
- (4) **Discovery of firearms and ammunition.** For definition and classification of firearms, Chapter 2 of the Weapons Act must be taken into account: <https://www.riigiteataja.ee/en/eli/ee/506082018003/consolide/current>. For definition and classification of ammunition, Chapter 2 of the Weapons Act has to be taken into account. If a weapon or ammunition is discovered on a ship or in a port facility and there is suspicion that their carriage was intended for the purpose of endangering passengers, crew or the ship, and further action is initiated (e.g., confiscation of the weapon, notification of the Police and Border Guard Board), this must be reported to the Estonian Transport Administration within 24 hours.
- (5) **Discovery of explosives component parts.** This incident type includes the discovery of the component parts of an explosive device such as the detonator. For obvious reasons batteries are not considered to be a part of an explosive device unless there are other components present. Where the discovery of such components involves suspicion that their carriage was intended for the purpose of endangering passengers, crew or the ship, and further action is initiated (e.g. by the Estonian Police and Border Guard Board, Estonian Rescue Board), this should be reported to the Estonian Transport Administration within 24 hours.
- (6) **Unauthorized access to Restricted Areas.** This incident type covers all cases when an individual gains an unauthorized access to a Restricted Area within the ship or port facility. Where an unauthorized access involves suspicion that the access was intended for the purpose of endangering passengers, crew or the ship, and further action is initiated (e.g. information submitted to the Estonian Police and Border Guard Board, a full ship or port facility search initiated), this must be reported to the Estonian Transport Administration immediately.
- (7) **Hijack.** The hijack of any ship must be reported to the Estonian Transport Administration immediately.

- (8) Unauthorized entry of a vessel into the port waters.** If it is discovered that a vessel or small craft has entered the port's waters without authorization, the Joint Rescue Coordination Centre Tallinn (JRCC TALLINN) must be notified immediately. Estonian Transport Administration must be notified within 24 hours.
- (9) Unauthorized operation of an unmanned aerial vehicle (UAV).** If an UAV is detected operating over restricted areas of the port facility without prior authorization from the port authority, Estonian Transport Administration must be notified within 24 hours.
- (10) Cyber incident.** A cyber incident is a situation in which the confidentiality, integrity, or availability of an organization's, institution's, or individual's information system and/or the information contained therein is compromised. Cyber incidents also include situations where another person's information system is used without authorization or its operation is intentionally disrupted. Notifications to the Estonian Information System Authority (CERT-EE) regarding a cyber incident must be submitted via the online portal raport.cert.ee or by email at cert@cert.ee. A cyber incident that affected the operation of the ship or the port facility must be reported to the Estonian Transport Administration within 24 hours.
- (11) Other security incidents.** If the ship security officer, company security officer or port facility security officer considers it necessary to inform the Estonian Transport Administration of any other security incident, this must be done as they consider appropriate.

Scheme “Reporting the security incidents”

When immediate notification of a security incident is required, the Vessel Traffic Management Department of the Estonian Transport Administration must be informed at first by phone and then by e-mail.

Incidents which require notification within 24 hrs may be reported to the Vessel Traffic Management Department of the Estonian Transport Administration only by e-mail.

Incident type	Immediate notification	Notification within 24 hrs
Serious bomb threats	X	
Discovery of explosives	X	
Incidents of which media are aware	X	
Discovery of firearms and ammunition		X
Discovery of explosives component parts		X
Hijack	X	
Unauthorized access to restricted areas	X	
Unauthorized entry of a vessel into the port waters		X
Unauthorized operation of an unmanned aerial vehicle		X
Cyber incident		X
Other incidents	As considered appropriate	

The contact details of the Vessel Traffic Management Department of Estonian Transport Administration

Phone: +372 6205 665

E-mail: maritime.security@transpordiamet.ee

The contact details of the Joint Rescue Coordination Centre Tallinn (JRCC TALLINN)

Phone: +372 619 1224

E-mail: jrcc@politsei.ee