

1 March 2022

Terms of Use – Cybersecurity Label for IoT consumer devices

1 Cybersecurity Label

The Finnish Transport and Communications Agency Traficom's Cybersecurity Label indicates that the labelled product or service is designed to be secure. The Cybersecurity Label is only issued to products and services that meet the information security requirements set by the National Cyber Security Centre Finland at Traficom. For organisations, the Cybersecurity Label is a simple way to communicate responsibility and to indicate that security is taken into account in the design of their products.

2 Use of the Cybersecurity Label

The Finnish Transport and Communications Agency Traficom owns the visual Cybersecurity Label trademark and grants it to organisations upon application. The application form and the related instructions are available on the website www.tietoturvamerkki.fi. Further information about the Cybersecurity Label can be requested by email at cybersecuritylabel@traficom.fi.

The validity period of the Cybersecurity Label can be specified at the start of the application process. The validity period may not exceed the period during which security updates are provided for the product¹.

When applying for the Cybersecurity Label, the organisation shall pay Traficom EUR 350 per product/service per label granted. This amount will not be refunded even if the device or service fails to meet the requirements. In connection with the application process, the organisation also pays the costs of auditing the products or services. After a product or service has been granted the Cybersecurity Label, the right of use and maintenance costs charged for the label are EUR 350 per product/service per year. The charge for the right of use and maintenance costs includes the annual audit. An organisation may stop using the Cybersecurity Label by notifying Traficom of its decision.

Traficom maintains a list of organisations and products that have been granted the Cybersecurity Label. Traficom may prohibit an organisation from using the label if the organisation fails to meet the obligations pertaining to its use. In that case, Traficom also removes any information about the product from the website www.tietoturvamerkki.fi and informs the public separately, if necessary.

After receiving the right to use the Cybersecurity Label in connection with a specific product or service, an organisation may use the label in various ways for marketing, communication and sales purposes.

The Cybersecurity Label is only issued for the products or services for which it has been applied, and it may not be used in connection with the organisation's other products. The use of the label is monitored by means of spot checks and feedback received, for example.

Traficom shall not be liable if an organisation uses the Cybersecurity Label in violation of the law or good practice.

¹ In certain cases, it may be possible that a product does not contain components that require the device to be updated against security issues over the course of its life cycle. However, updating the product should be made possible and performed, if necessary.

1 March 2022

These Terms of Use may be changed as deemed necessary by Traficom, for example, in the event of legislative developments. Traficom will publish information on any changes to the Terms of Use on its website. Traficom reserves the right to modify and/or update the content of the Cybersecurity Label or to prevent the use/distribution of the Cybersecurity Label. The changes may not require the organisations that have been granted the Cybersecurity Label to make unreasonable changes to the relevant products or services during the validity period of the label granted to them.

Further instructions on using the Cybersecurity Label are provided in the appendix "Graphic image of the Cybersecurity Label", which is provided to the organisation after granting the label.

3 Organisation's obligations

An organisation whose product or service has been granted the Cybersecurity Label is required to notify Traficom of any security breaches and other problems that could compromise the security of a product or service bearing the Cybersecurity Label. Such problems include, for example, previously unknown vulnerabilities. The organisation must notify Traficom without delay once the issue has come to the organisation's attention. Notifications must be sent by email to cybersecuritylabel@traficom.fi. After becoming aware of the issue, Traficom and the organisation discuss the nature of the problem and jointly agree on a schedule for corrective action. Typically, corrective action must be taken within a maximum of 90 days.

The organisation must also inform Traficom of any updates or changes to a product or service to which Traficom has granted the Cybersecurity Label if the updates or changes may have a material impact on the information security features of the product or service. In that case, Traficom may review the changes.